NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

KOINONIA: THE REQUIREMENTS AND VISION FOR AN UNCLASSIFIED INFORMATION-SHARING SYSTEM

by

Nathan A. Rao
Oscar W. Simmons

June 2013

Thesis Advisor:	Alex Bordetsky
Second Reader:	Ray Buettner

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704–0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** June 2013	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE KOINONIA: THE REQUIREMENTS AND VISION FOR AN UNCLASSIFIED INFORMATION-SHARING SYSTEM	**5. FUNDING NUMBERS**
6. AUTHOR(S) Nathan A. Rao, Oscar W. Simmons	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943–5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

This thesis examines requirements necessary to build a collaborative information-sharing system for future war or actions other than war with international, coalition, and Non-Government Organization partners. Theater Special Operations Commands, and more specifically, Special Operations Command Europe, constantly work with partner nations and desire this capability. Much of this work is relevant for NATO Special Operations Forces. Additionally, this thesis examines potential solutions for a collaborative ISR system.

14. SUBJECT TERMS NATO SOF, NSCC, NSHQ, Special Operations Interoperability, Military Networks, NATO Transformation, European Common Threats, NATO Training and Education Program-NSTEP, Intelligence Sharing, Multinational Operations, Intelligence, Coalitions.	**15. NUMBER OF PAGES** 83
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

THIS PAGE INTENTIONALLY LEFT BLANK

KOINONIA: THE REQUIREMENTS AND VISION FOR AN UNCLASSIFIED INFORMATION-SHARING SYSTEM

Nathan A. Rao
Lieutenant, United States Navy
B.A., University of Pennsylvania, 2007

Oscar W. Simmons
Lieutenant Commander, United States Navy
B.S., Excelsior College, 2001

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS TECHNOLOGY
(COMMAND, CONTROL, & COMMUNICATIONS)

from the

NAVAL POSTGRADUATE SCHOOL
June 2013

Authors:	Nathan A. Rao Oscar W. Simmons
Approved by:	Dr. Alex Bordetsky Thesis Advisor
	Dr. Ray Buettner Second Reader
	Dr. Dan Boger Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis examines requirements necessary to build a collaborative information-sharing system for future war or actions other than war with international, coalition, and Non-Government Organization partners. Theater Special Operations Commands, and more specifically, Special Operations Command Europe, constantly work with partner nations and desire this capability. Much of this work is relevant for NATO Special Operations Forces. Additionally, this thesis examines potential solutions for a collaborative ISR system.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

NCE	Non-Classified Environment
IGO	Intergovernmental Organization
NGO	Non-government Organization
DoD	U.S. Department of Defense
DISA	Defense Information Systems Agency
ISR	Intelligence, Surveillance, and Reconnaissance
NSA	National Security Agency
DHS	Department of Homeland Security
DoS	Department of State
EUCOM	U.S. European Command
PACOM	U.S. Pacific Command
SOCEUR	Special Operations Command Europe
CENTRIX	Combined Enterprise Regional Information Exchange System
BICES	Battlefield Intelligence Collection Exploitation System
SIPRNet	Secure Internet Protocol Router Network
NIPRNet	Non-classified Internet Protocol Network
GIG	Global Information Grid
U.S.	United States
TNT	Tactical Network Testbed
MIO	Maritime Interdiction Operations
NORNAVSOC	Norwegian Naval Special Operations Command
AIS	Automatic Identification System
SOCOM	U.S. Special Operations Command
JCBRND	Joint Chemical, Biological, Radiological, Nuclear Defense
MDSRP	Maritime Defense and Security Research Program
CoE	Center of Excellence

SOF	Special Operations Forces
SA	Situational Awareness
COP	Common Operating Picture
CoT	Cursor on Target
APAN	All Partners Access Network
REL-DMZ	Releasable De-Militarized Zone
NOFORN	Not Releasable to Foreign Nationals
PKI	Public Key Infrastructure
OSI	Open Source Intelligence
GSM	Global System for Mobile
3G	Third generation of mobile telecommunications technology
VTC	Video Teleconference
TISC	Transnational Information Sharing Cooperation
JCTD	Joint Concept Technology Demonstration
FY	Fiscal year
RSS	Really Simple Syndication
SMS	Simple Message Service
MMS	Multimedia Message Service
UIS	Unclassified Information Sharing
UISS	Unclassified Information Sharing Service
ES	Enterprise Service
C2	Command and Control
OTHTTS	Over The Horizon Tactical Tracking System
MCCIS	Maritime Command and Control Information System
OSD	Office of the Secretary Of Defense

CAPE	Director for Cost Assessment Program Evaluation
DOT&E	Director, Operation Test and Evaluation
JCIM	Joint Civil Information Management
JT&E	Joint Test and Evaluation
TTP	Techniques Tactics and Procedures
CIM	Civil Information Management
COTS	Commercial Off-The-Shelf
FMN	Future Mission Network
SOA	Service Oriented Architecture
XML	Extensible Markup Language
CWIX	Coaltion Warrior Interoperability eXploration, eXperimentation, eXamination, eXercise
ON	Observer Notepad
XMPP	Extensible Messaging and Presence Protocol

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

The authors would like to thank the following people whose assistance, support, and contributions made this thesis possible:

I would be remiss if I did not first thank Alex Bordetsky, my advisor, for inviting me to the lab and introducing the experimentation from ongoing research that proved so useful. Your guidance and patience made this work possible, and your unfailing enthusiasm was a buoy when we encountered obstacles.

I am indebted to Professor Ray Buettner, also of the Naval Postgraduate School, for introducing the ideas and concepts that were of current practical interest and for guiding their development into a worthwhile opportunity.

My deepest appreciation is due to my wife, Laura, an excellent wife and mother. Her loving support made this work possible. I dedicate this thesis to our children, Maria, Elizabeth, and Nathan. It is good to come home to your smiles.

—Nathan Rao

I echo Nate’s sentiment for Alex Bordetsky. His invaluable understanding, patience, and direction led to completion of a thesis I did not think possible. From our initial discussions to concept development to nailing down specifics, he proved himself a warm and receptive academic willing to talk us through our problems and guide us to reasonable solutions. I always left his office in a better state than when I entered it.

To Ray Buettner, thank you for planting the seed of an idea and opening our minds to think beyond the typical canned responses. Thank you for opening our minds to go beyond the written requirements and see the interplay of small parts into greater systems. Thank you for presenting me with writings to challenge my concepts and forcing me to codify my ideas. It is the road less traveled, and it has made all the difference.

To my beloved wife Reihi, thank you for putting up with me and supporting me through last-minute phone calls and long days. Unfortunately, our future will require no less challenge, but I look forward to the ride. And to my children, of whom I love to brag, thank you for giving me so much material.

—Oscar Simmons

I. INTRODUCTION

> The foundation of United States, regional, and global security will remain America's relations with our allies, and our commitment to their security is unshakable. These relationships must be constantly cultivated, not just because they are indispensable for U.S. interests and national security objectives, but because they are fundamental to our collective security. Alliances are force multipliers: through multinational cooperation and coordination, the sum of our actions is always greater than if we act alone....we will continue to mutually benefit from the collective security provided by strong alliances.
>
> —President Barack Obama
> (Office of the President of the United States 2010)

In alignment with executive guidance, the U.S. military is increasingly engaged in collaboration with non-traditional coalition partners, such as non-governmental organizations (NGOs), intergovernmental organizations (IGOs), and foreign military, governmental, and civilian organizations. The Department of Defense (DoD) is also expanding its collaboration with other U.S. departments and agencies which are critical to success in many operations other than war, and in security cooperation efforts. This paper will discuss the requirements for a proposed unclassified information sharing system suitable for use in missions that involve U.S. military cooperation with partners that either cannot communicate intelligence, surveillance, or reconnaissance (ISR) information at a classified level, or which could accelerate the sharing of information to augment classified networks with a more agile, albeit limited, data path.

A. BACKGROUND

The requirement for a basic ISR sharing system originated with Special Operations Command Europe (SOCEUR), where General Repass (U.S. Army) identified it as a priority (McMullen 2012). He wanted the ability to share ISR data with coalition partners in United States European Command (EUCOM) with whom U.S. ISR data could not currently be shared. The informal name of this required system was “Blue Collar ISR,” a temporary term chosen to connote that this desired information sharing system did not need to have extensive capability but instead was intended to satisfy basic ISR data-sharing needs with theater partners who had budgetary constraints and capability limitations. Dr. Raymond Buettner traveled to Stuttgart, Germany, learned of this requirement, and shared it with us, leading us to begin thinking about the problem.

1. Classification

One of the first attributes of this information-sharing system that we discussed was the highest level of classification necessary. Our initial impression from personal experience with current practice was that U.S. ISR information is usually classified Secret. That classification poses a very significant challenge to sharing with potential foreign partner nations and NGOs. Some partner nations hold most of their ISR data at the Confidential or Restricted level and have limited systems able to process Secret information and few personnel with the requisite clearance. Other potential partners, such as NGOs, may have no capability to process classified information. Nations that have significant capability to process classified information are not those for whom a “blue collar” ISR solution is needed. The U.S. can already share such data over CENTRIX (Combined Enterprise Regional Information Exchange System), BICES (Battlefield Intelligence Collection Exploitation System), or other existing, more robust, systems, and the addition of a “blue collar” system with less capability than provided by existing networks would be redundant (Wills 2012).

2. Enterprise Purpose

Since this network is conceived of as supporting specific missions of limited duration rather than as a major national network for communicating with permanent allies, such as NATO member states, it is helpful to define the enterprise under consideration as small and tactical, designed to be rapidly deployed in missions where time agility is critical (North Atlantic Treaty Organization Special Operations Coordination Centre 2008). A likely example of a U.S. military unit that might deploy this network would be a Joint Special Operations Task Force (JSOTF), a tactical unit subordinate to one of the Theater Special Operations Commands (TSOC) which in turn support one of the six geographic Combatant Commanders (US Department of Defense 2007).

B. THE PROBLEM

General James Cartwright wrote *Information Sharing as a Strategic Imperative* in 2006, highlighting the necessity of a culture shift away from “need to know” toward “need to share:” “Success in today’s environment requires effectively coordinating all intelligence collection capabilities. The information collected must then be made available to a wide range of customers based on a secured need-to-share basis rather than the old need-to-know threshold” (J. E. Cartwright 2006).

The problem this thesis addresses is the challenge of sharing relevant but unclassified ISR or other information with coalition partners, which include not only foreign militaries, but IGOs, NGOs, and others, depending on the mission.

> The 9/11 Commission’s conclusions as to intelligence-sharing within the U.S. intelligence community apply equally to intelligence-sharing with foreign liaison services: “Current security requirements nurture overclassification and excessive compartmentalization of information among agencies. Each agency’s incentive structure opposes sharing, with risks (criminal, civil, and internal administrative sanctions) but few rewards for sharing information.” Undersecretary of Defense for Intelligence Stephen Cambone recognized this problem within the Defense Department and issued a memo to defense intelligence agencies that stated, “Incorrect use of the NOFORN [U.S.-only consumers] caveat on DoD information has impeded the sharing of classified national defense information with allies and coalition partners.” Cambone subsequently prescribed new means to ensure the widest dissemination of intelligence information and demanded that for “intelligence under the purview of the DoD, originators shall use the ‘Releasable to’ (rel to) marking, and any subsequently approved releasability marking to the *maximum extent possible*.” In the war on terror, sharing is the norm. (Reveron 2006)

1. What Isn’t Working in the Current Paradigm

The current way that the U.S. tends to handle most intelligence data is to import it all to SIPRNet once it is gathered. This is the domain that U.S. military intelligence analysts use for most of their work, and the necessity of having at least a Secret security clearance to access the network is no impediment since they all have at least that level of clearance. SIPRNet supports information that is Secret or below, so working on that network permits the inclusion of unclassified data, since data of lower levels of classification can easily move to a domain of a higher classification, it just cannot flow in the other direction. When information on SIPRNet needs to be shared with a foreign coalition partner nation, as it often is in EUCOM, then use is made of tools like DISA (Defense Information Systems Agency) Europe’s Releasable De-Militarized Zone (REL-DMZ), a region of SIPRNet from which NOFORN information is excluded and where partner nations with Secret networks can access Secret Releasable data from their Secret network by means of an intermediate cross domain guard, or gateway.

C. LIMITATIONS AND SCOPE

Mission sets such as Humanitarian Assistance or Disaster Relief (HA/DR) often require an information sharing solution that can be deployed to remote locations and achieve operational capability very quickly to facilitate communication between governmental and non-governmental organizations from various nations during the initial hours after a disaster. A hypothetical network designed to meet these purposes will be small and limited in scope of users and size of infrastructure to the mission, and it will be designed to operate for a limited duration.

Overall, the attributes of this hypothetical network that must be considered are:

- Purpose/Mission
- Classification

- Access
- Duration
- Mobility
- Duration
- Mutual Benefit
- Centralized Decision Making
- Trusted Network
- Data Inputs
- Technology
- Interoperability

For brevity, we will give a name to the proposed network that addresses these requirements. *Koinonia* is a classical term that refers to sharing, or participation in a shared endeavor, and so we will name our hypothetical network with a word that describes its purpose. Koinonia, then, is a notional network that is conceived of as other than a U.S. national network. This network cannot exist as an exclusively U.S. classified network. As defined in the latest Intelligence Community Classification Guidance Findings and Recommendations Report:

> Thus, according to the President of the United States, only information owned by, produced four, or under the control of the U.S. government that could cause harm if disclosed in an unauthorized manner and contained in one of the eight categories above may be classified. (Director of National Intelligence and Chief Information Officer 2008)

It may be desirable to have a network that is not an exclusively military or federal government network. When the federal government is a partner with other organizations, the information resident within a connecting network may need to be unclassified. Sensitive but unclassified data is the type of information used by Regional Information Sharing Systems (RISS) Secure Intranet

(RISSNET), and the RISS Automated Trusted Information Exchange (RISS ATIX). The DOJ’s (Department of Justice) Law Enforcement Online (LEO) network is sensitive but unclassified, as is the Department of Homeland Security’s (DHS) Federal Protective Service (FPS) Secure Portal System, and their flagship Homeland Security Information Network (HSIN), with its thirty-five communities of interest (United States Government Accountability Office 2007).

II. RELATED WORK AND LITERATURE REVIEW

Information sharing has been a challenge for coalition operations for as long as different organizations have attempted to cooperate. Developments in technologies have not always eased the challenge, but military doctrine and case studies point out ways to mitigate the difficulty. The following doctrinal publications and studies will be reviewed in this chapter.

Title	Topic
Joint Intelligence Publication 2–0	Joint Intelligence
Joint Intelligence Publication 2–01	Joint and National Intelligence Support to Military Operations
Joint Intelligence Publication 3–05.1	Joint Special Operations Task Force Operations
Help a Brother Out: A Case Study and Multinational Intelligence Sharing, NATO SOF	Building keys to sharing intelligence in NATO Special Operations
Case study: Intelligence – Open-source data analytics	Cost savings and analytics in using social networking.
On Facilitating Stability Operations: a Net Centric, Federated Approach to Information Sharing	Use of APAN for unclassified information sharing.
Testbed for Tactical Networking and Collaboration	A testbed environment for sharing technologies

Table 1. References for related work.

A. JOINT OPERATIONS

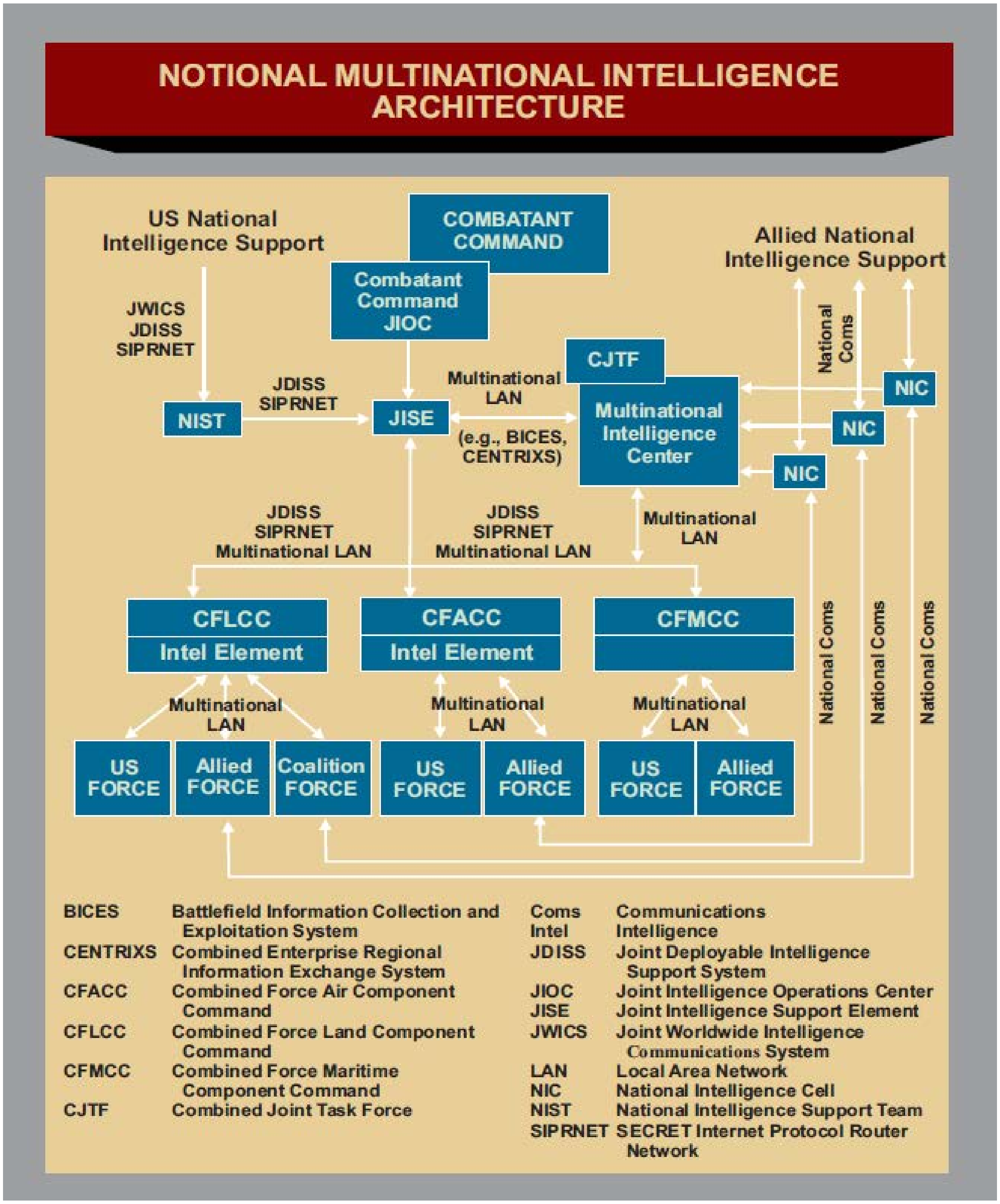
Military doctrine is codified in publications which serve as a foundation for any work on the subjects they address. Our analysis of requirements and goals begins with joint doctrine.

1. Joint Intelligence Publication 2–0

The Joint Intelligence Publication outlines very clearly the goals and requirements for joint, interagency, and multinational intelligence sharing and cooperation:

> Being faster and better requires having unfettered access to the collection, processing, and dissemination of information derived from all available sources. Information sharing, cooperation, collaboration, and coordination are enabled by an intelligence and information sharing environment that fully integrates joint, multinational, and interagency partners in a collaborative enterprise. This type of collaborative intelligence sharing environment must be capable of generating and moving intelligence, operational information, and orders where needed in the shortest possible time. The architecture supporting this type of environment must be dynamic, flexible, and capable of providing multinational partners and interagency participants rapid access to appropriate data. It must facilitate the capability of the IC to focus on supporting the JFC and subordinate joint force components and to integrate support from non-DoD agencies and NGOs as needed. (U.S. Department of Defense 2007)

Many salient points to our topic can be derived from this paragraph. The first of which is the importance of sufficiently inclusive access. The use of terms like “unfettered access” in the context of joint intelligence doctrine highlights the great importance of overcoming roadblocks to getting necessary information to partners in operations, as opposed to treating useful information as a resource that becomes more valuable to its possessor the more tightly the secret is protected from partners or competing intelligence communities. That access enables full participation of our partners through a better understanding and better ability to collaborate on a topic. Simply, the more they know the more they can participate. The second point concerns the necessity of an information sharing enterprise that facilitates collaboration beyond DoD borders. Such collaboration can only occur when there exists a system by which all of the different parties can come together to work on a topic. The nature of military information dictates that the enterprise will require a certain degree of security, but the security requirement cannot be permitted to override the requirement that the enterprise also be flexible and accessible. It necessary to consider how availability to all collaborating parties can best be extended with the desired amount of information offered, without compromising classified information or jeopardizing information assurance.



BICES	Battlefield Information Collection and Exploitation System
CENTRIXS	Combined Enterprise Regional Information Exchange System
CFACC	Combined Force Air Component Command
CFLCC	Combined Force Land Component Command
CFMCC	Combined Force Maritime Component Command
CJTF	Combined Joint Task Force
Coms	Communications
Intel	Intelligence
JDISS	Joint Deployable Intelligence Support System
JIOC	Joint Intelligence Operations Center
JISE	Joint Intelligence Support Element
JWICS	Joint Worldwide Intelligence Communications System
LAN	Local Area Network
NIC	National Intelligence Cell
NIST	National Intelligence Support Team
SIPRNET	SECRET Internet Protocol Router Network

Figure 1. Notional Multinational Intelligence Architecture (From U.S. Department of Defense 2007).

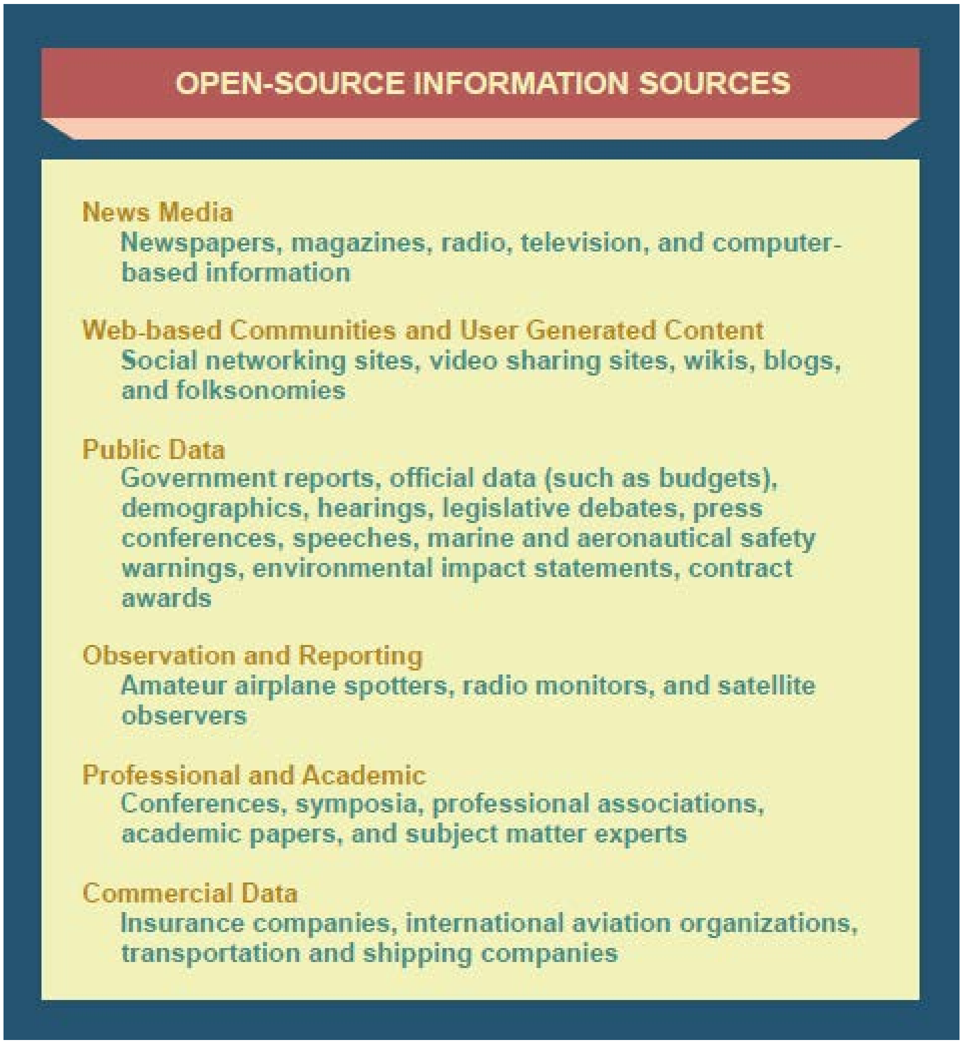
Examining the notional multinational intelligence architecture, shown in Figure 1, one can see several critical links labeled Multinational LAN. This implies the existence of a network available to all partners as it exists inside the staff planning loop, as well as outside, connecting U.S. and allied forces; however there is no specific system or network purpose-built to handle this job for all missions. Note that the diagram refers to “Multinational LAN” even more frequently than to U.S. classified networks. Given such importance, it is noteworthy that no single system exists to serve this role. Instead of being designed for a given mission, networks are customized for a specific set of participating nations, and if those participants change, a new network with a potentially new classification may be necessary. BICES and the various enclaves of CENTRIX, for example, are classified networks that cannot dynamically adjust to changing partner nation participation in a given mission and lack the flexibility to accommodate participation by partners that communicate exclusively at the unclassified level.

Personal experience has shown that in the absence of a network designed as a flexible multinational LAN, great efforts are made to extend access to U.S. classified networks to a very select group of partner nations, while all other allied forces are left out of the network and must solicit hand-me-down reports from those with access. Although this approach permits the exchange of classified data, the access limitations attendant to this capability necessarily result in a network that does not fit the requirements of a collaborative sharing environment called for in Joint Intelligence Publication 2–0. It does not allow all partners rapid access to appropriate data.

Further, the requirements stipulate the capacity to integrate nonmilitary agencies and organizations. In much the same manner, there is no dedicated system or network by which these organizations can collaborate with the U.S. military. Attempts have been made to overcome the shortfall. The All Partners Access Network (APAN), for example, was originally built for just such a purpose. Despite adoption at the national level after its initial success in PACOM, APAN has not seen worldwide utilization. This will be further evaluated in a later section.

2. Joint Intelligence Publication 2–01

While there is unquestionably a great deal of information which is appropriately classified, maintained on U.S. classified networks, and therefore cannot be shared, interagency and multinational partnerships require us to look for options and materials which can be shared on a multinational LAN capable of processing material which could be jointly accessed and shared in multinational and multi-organizational operations. We narrow the problem scope by looking at the individual components that provide for joint intelligence. The *Joint Publication 2–01, Joint and National Support to Military Operations*, outlines a type of intelligence which is available to all parties: Open Source Intelligence (OSINT) (U.S. Department of Defense 2012). Figure 2 lists many of the open-source information sources, all of which are unclassified and available to all members of any coalition operation in which the U.S. military might participate.



OPEN-SOURCE INFORMATION SOURCES

News Media
Newspapers, magazines, radio, television, and computer-based information

Web-based Communities and User Generated Content
Social networking sites, video sharing sites, wikis, blogs, and folksonomies

Public Data
Government reports, official data (such as budgets), demographics, hearings, legislative debates, press conferences, speeches, marine and aeronautical safety warnings, environmental impact statements, contract awards

Observation and Reporting
Amateur airplane spotters, radio monitors, and satellite observers

Professional and Academic
Conferences, symposia, professional associations, academic papers, and subject matter experts

Commercial Data
Insurance companies, international aviation organizations, transportation and shipping companies

Figure 2. Open-Source Information Sources (From U.S. Department of Defense 2012).

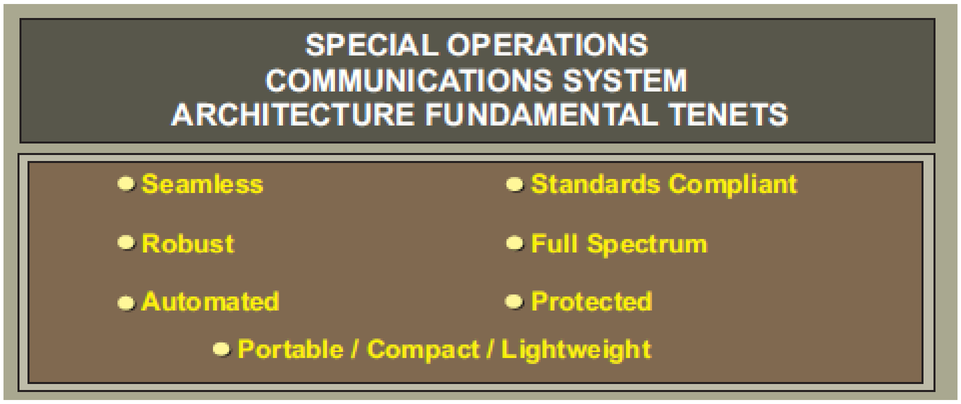
Web-based communities and user-generated content are especially significant, since social networking, video sharing, wiki, and blog sites may easily be interacted with on an unclassified network connected to the public internet. These information sources may be very valuable to a multinational or inter-agency network.

3. Joint Intelligence Publication 3–05.1

a. Communications Systems Support

A primary requirement for communications among SOF forces is interoperability. They must have the ability to interact with conventional forces, government organizations, NGOs, and IGOs. This may entail the use of not only state-of-the-art systems, but also less sophisticated systems, in an effort to maximize collaboration and communication of joint parties (US Department of Defense 2007). Frequently multiple alternative communication systems can be used to accomplish this task; however, simplifying the overall scheme of communications is always best, as it minimizes the technological support burden and risk of failure.

The fundamental architectural tenants of SOF communications expand upon this idea. Highlighted in Figure 3, and especially important when dealing in coalition communications, are the tenants of seamless architecture, standards compliance, and protected communications. These tenets will apply directly to the architecture of Koinonia, since a network built to facilitate broad information sharing may fail if there are capability gaps that prevent interoperability, or if standards are either not defined or not followed, or if compromise turns the network into a liability.



SPECIAL OPERATIONS
COMMUNICATIONS SYSTEM
ARCHITECTURE FUNDAMENTAL TENETS

- Seamless
- Standards Compliant
- Robust
- Full Spectrum
- Automated
- Protected
- Portable / Compact / Lightweight

Figure 3. Special Operations Communication System Architecture Fundamentals Tenants (From US Department of Defense 2007).

b. Information Management

There are three forms in which digital information should be managed: information sharing, collaboration, and force tracking. Information sharing, while it may have a tangible aspect, can be more readily accomplished by electronic means, potentially promoting efficiency and aiding synchronization of effort. Collaboration requires that the shared information be held in such a manner that multiple parties can contribute to its development and plan from it. Force tracking, usually done via a Common Operational Picture (COP), improves situational awareness and supports the expeditious and accurate granting of clearance for fires, as well as reducing the need for friendly units to pass their position verbally (US Department of Defense 2007).

In combat operations, information is kept on classified networks. This is justified, as it protects people, data, and planning from hostile actions. However, in operations other than war, the ability to share data can be extremely valuable when coordinating across multiple organizations and nationalities. Further, disparate types of data need not be held on the same domain. For example, force tracking may be conducted on a classified network, while information-sharing collaboration can be performed on a multinational LAN. The placement of the information should be on the network that provides the greatest advantage for the coalition forces without entailing excessive risk.

B. HELP A BROTHER OUT

> This thesis examines how to optimize intelligence sharing in a coalition by a thorough literature review and site visits to intelligence sharing organizations in order to establish best practices for multinational intelligence sharing. The newly established NATO SOF Headquarters (NSHQ) in Mons, Belgium was treated as a test case to validate their intelligence sharing procedures and structures in reference to the authors' identified best practices: mutual gains and benefits; trust; direct control; and accessibility and interoperability.
>
> Intelligence support to SOF is a *decisive* factor, when in conventional operations it often is not; therefore intelligence support to SOF is special - NATOSOF is no exception. The level of intelligence support to SOF normally only exists at the national

> level, due to bureaucratic obstacles, a need to protect sensitive sources and capabilities, and lack of trust. The NSHQ is experimenting with several innovative methods to enhance trust and streamline intelligence capability amongst NATO SOF forces. There are structural and organizational lessons learned from the establishment of the NSHQ that can be applied to future operations and coalitions. (Ara, Brand and A 2011)

The work that NATO is doing within the realm of collaboration is relevant to finding the requirements and solution sets for coalition information sharing. In this humorously titled thesis, NATO officers looked up processes which could improve information sharing and processes which could be valuable in any collaborative situation involving multiple nations and organizations. In their study, they found five keys to increasing the efficiency of intelligence support to SOF forces

1. Mutual Benefit from Coalition Membership

There is a benefit of improved force effectiveness when partner nations collaborate towards a common goal. The argument is not that the combination produces a necessarily better product, but that when trying to rely on a single national domain, gathering the intelligence can be time-consuming, problematic, and potentially unreliable for other nations. It is simply too hard for others to get and share if information belongs to just one nation. Rather, if you build your intelligence as a partnership it becomes faster and easier to access, and more reliable (Ara, Brand and A 2011).

2. Trust and Competency Established Among the Members

Repetitive training exercises and common training programs have resulted in frequent collaboration amongst NATO’s relatively small SOF community. This repeated contact allows a buildup of trust amongst personnel, as well as, (and perhaps more importantly than) trust in the capabilities of partner nations. When partners are united by a common goal and share the workload, creating an enterprise by which to share information can become much easier (Ara, Brand and A 2011).

3. Centralized Decision Making

The capabilities and influence of the United States can support standardization for multinational requirements and benchmarks. Processes can begin with those previously established by the U.S. and capabilities can be expanded by mimicking those that are or are being developed. A federated approach to network management is promising (Ara, Brand and A 2011).

4. Increased Use of COTS Equipment and Open Source Information

Advocating the use of immediately accessible technology, through commercial off-the-shelf (COTS) equipment and open source information, will help to fill the gaps present in the NATO SOF networks (Ara, Brand and A 2011). In 2007, most NATO SOF units did not have access to NATO systems at the headquarters or tactical levels. The BICES system was selected for the classified NATO network (Dron 2009). Several examples are used to illustrate the cost-effective use of COTS and of secured but unclassified data stores. Obtaining inexpensive equipment and using it at the local level has improved their efficiency by cutting out the bureaucracy in dealing with national level systems (Ara, Brand and A 2011).

5. Secure or Trusted Network

Realizing there is no easy access to national level intelligence services; NATO SOF increased their effectiveness by building homegrown capabilities. These have been modeled after individual national systems, which are already in place. By placing it at a level where it is accessible to all coalition forces, the information on the system is made relevant to the operators (Ara, Brand and A 2011). This is effectively shown in the words of Gen. David Petraeus, in an address to the NATO Secretary General:

> Over the past three months, SOF elements carried out more than 4,000 total operations that captured or killed 235 insurgent leaders and more than 2,500 lower-level fighters – likely an unprecedented number in the history of SOF. The increase in SOF successes also

> results from improved ISR capabilities, our improved abilities to fuse intelligence, increased partnering efforts with Afghan Special Forces, and improved capabilities of our Afghan SOF partners. (Petraeus 2010)

C. ALL PARTNERS ACCESS NETWORK (APAN)

Catastrophes around the globe which call upon humanitarian assistance and disaster relief efforts require a collaborative environment for the various military and civilian responders. One such environment comes in the form of the All Partners Access Network. As an unclassified work, analyzing the APAN program proves a valuable resource for indicating requirements and solutions for a multinational, multi-organization operation

1. Background

Evidenced in the aftermath of the Indian Ocean Basin Tsunami of 2004, the U.S. DoD required a method for sharing unclassified information amongst the variety of government and nongovernment organizations and militaries cooperating on casualty response (Chlebo, Christman and Johnson 2011). Quickly realizing the traditional web was not enough, the Assistant Secretary of Defense for Networks and Information Integration informed his staff of the need to communicate, collaborate, translate, and engage in order to share unclassified information more readily and increase the overall effectiveness of the U.S. response (R. K. Ackerman 2006). This idea was a departure from the typical attempt to exercise command and control (C2) through classified networks. Given the state of the actors, classified networks were not a viable option (Chlebo, Christman and Johnson 2011).

The Unclassified Information Sharing (UIS) Enterprise Service (ES) is maturing in the “dot mil” network. However, its rigid structure and designed limitations fail to satisfy the requirements for responsiveness, and flexibility (Chlebo, Christman and Johnson 2011). Instead, a goal for Koinonia should be to enable agile C2 (Alberts and Hayes 2007) with an expanded set of possible partner entities. Alberts and Hayes go on to explore various C2 elements in a complex operational environment to provide a framework for emerging elements. Future C2 systems will rely on information shared in an unclassified environment, as there is a correlation between development of C2 systems and information sharing (Chlebo, Christman and Johnson 2011). Broad information sharing and collaboration with NGOs or non-allied nations, which may be necessary in complex endeavors, is only possible in an unclassified environment.

2. Early Unclassified Web Presence

APAN originated in the U.S. Pacific Command as part of an effort to share information with multinational partners in Multinational Planning Augmentation Team (MPAT) (Tempest Express Fact Sheet 2011). It was a simple website used for file sharing and a one-way publishing mechanism for posting publicly releasable information on exercises. The website gained portal features and became more operationally sensitive for impact members. At that time it was known as the Asian Pacific Access Network. It was in the assistance efforts after the tsunami in the Indian Ocean basin which showed the potential of the site, as it proved to be the only effective mechanism for the various responders to de-conflict their efforts (Chlebo, Christman and Johnson 2011).

3. Transnational Information Sharing Cooperation Joint Concept Technology Demonstration

The Transnational Information Sharing Cooperation (TISC) Joint Concept Technology Demonstration (JCTD) started in fiscal year (FY) 2007. Its goal is to foster information sharing amongst U.S. military, U.S. government and other less traditional mission partners by implementing social networking practices, capabilities, and concepts into a portal environment. Funding has been allocated to transition from a demonstration platform to a shared enterprise service available to Combatant Commands in support of unclassified operations. Capabilities are expected to include wiki, blog, chat, translation, geospatial information tools, advanced search, Word Cloud Maps, Single Sign-On, Really Simple Syndication (RSS), Simple Message Service (SMS) and Multimedia

Message Service (MMS). This provides Geographic Combatant Command (GCC) agility when the tools are partnered with policy authorities to engage in operations with nontraditional mission partners and an unclassified dot org environment. Information sharing between the dot org and dot mil environments allow for coordination and collaboration on critical issues (Chlebo, Christman and Johnson 2011).

4. JCTD to an Enterprise Service

The Office of the Secretary Of Defense (OSD) Director for Cost Assessment Program Evaluation (CAPE) directed DISA to implement the UIS ES for the DoD via Resource Memorandum Decision - 700. Requirements for the transition of the JCTD concept to an ES were vetted and approved by the DoD CIO. Putting aside further development of existing technologies, in order to use the service as planned, meets the requirements of the Clinger Cohen Act. In this way, the DoD CIO is realizing information technology efficiencies across the Department (Chlebo, Christman and Johnson 2011).

5. Network Design for an Agile UIS

A newly formed Stability Operations Community of Interest took a year to examine case studies, create a problem statement, and build a high level roadmap for capabilities (G. Christman 2009). A follow-on pilot program combined multiple services to demonstrate a conceptual model for comprehensive approach to civil-military information sharing (G. Christman 2010). This model is shown in Figure 5.

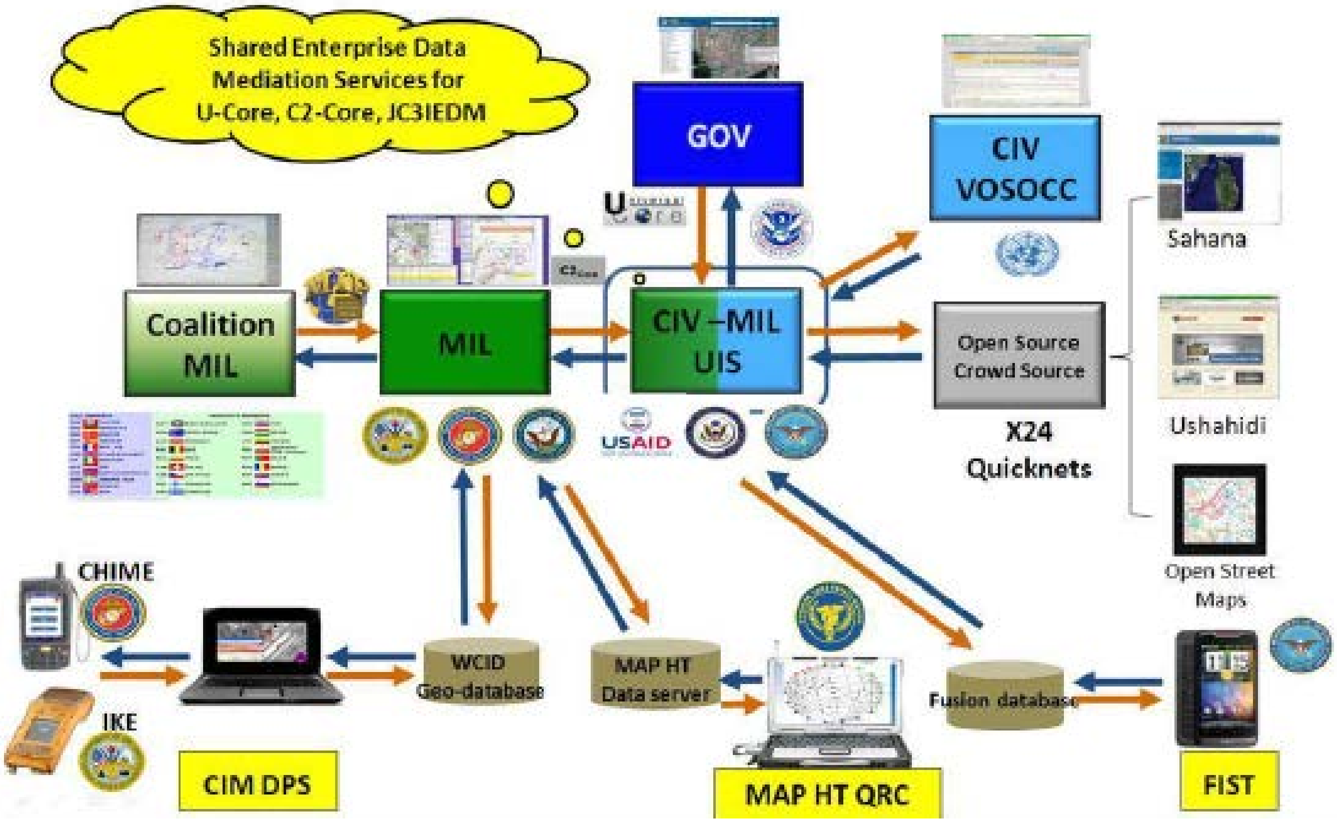


Figure 4. Conceptual model of a comprehensive approach to CIM information sharing (From Christman 2010).

The Director, Operation Test and Evaluation (DOT&E) published findings on the Joint Civil Information Management (JCIM) Joint Test and Evaluation (JT&E). The findings were used to produce the Techniques Tactics and Procedures (TTP) handbook for Civil Information Management (CIM) in order to standardize assessment methods and information management processes (Chlebo, Christman and Johnson 2011). The conceptual model from Figure 4 utilizes these findings. Further development of this concept has begun throughout the services. U.S. Special Operations Command (USSOCOM), the U.S. Army, and U.S. Marine Corps have all initiated programs for CIM (Chlebo, Christman and Johnson 2011).

6. Further Development

With connection points between the ".mil," ".org," and the".mil" domains, and data paths to NATO allies, the UIS can act as a hub for coalition operations. Leveraging work done in the pilot program with models constructed in the unclassified core enterprise (Chlebo, Christman and Johnson 2011) with further this growth. The mediation service must be developed in order to link these environments to leverage those pivot points (G. Christman 2010).

Three specific areas need to be developed in order to create a data-related hub from which to work. We discussed the first area in the open-source data mining section. It involves intelligent agent-based technologies and improved data mining methods in order to make the most of the data available in the UIS (Chisolm 2007). The second is consolidation of authoritative databases (Daniel, Goh and Yusop 2007). The third is to develop machine-readable data for use in a Service Oriented Architecture (SOA) and to apply Business Intelligence to determine where and what data is being pulled in order to best meet the needs of the customer (Hammergren and Simon 2009).

7. Meeting the Need for Information

The first step in undertaking any challenge is to understand the requirement and how to address it. However, unlike civilian businesses where the environment is generally steady, the military deploys into situations where the unknown far outweighs the known. The goal for information gatherers is to flip that ratio as quickly as possible. This concept is illustrated in the information versus time graph of Figure 5. The Haiti earthquake is an example of such a scenario in which the information gap prevented early and effective application of resources (Chlebo, Christman and Johnson 2011). The response to Haiti benefited from the rise of social media through crowdsourced crisis response (Hester, Shaw and Biewald 2010).

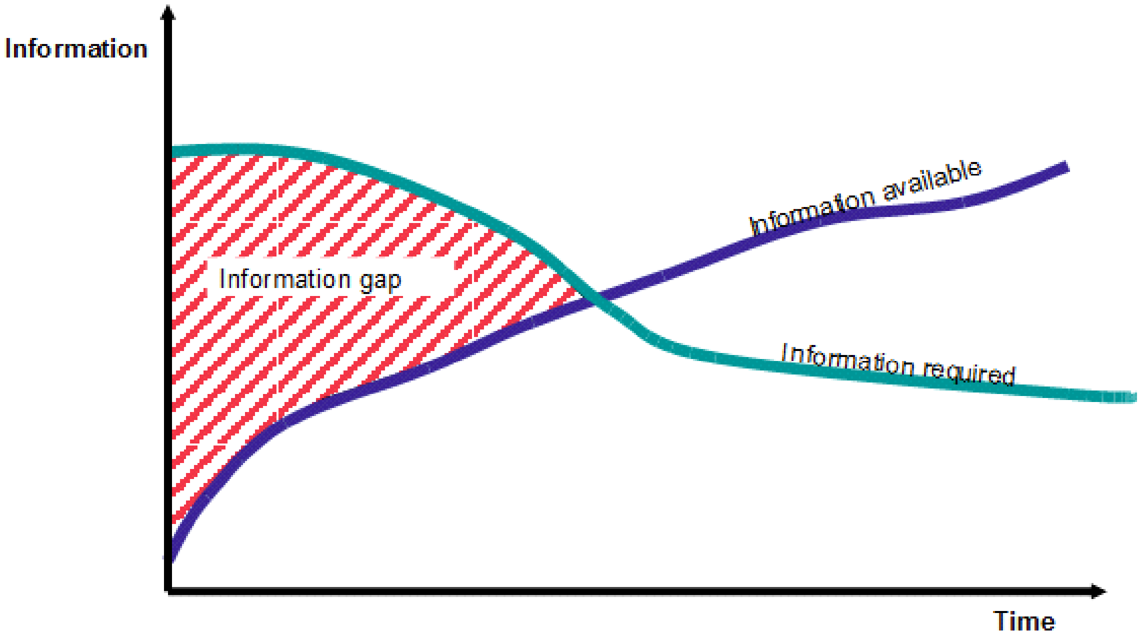


Figure 5. Illustration of available and required information over time (From Chlebo, Christman and Johnson 2011).

Data gathered through outsourcing over cellular tower networks can be used in several toolsets. As illustrated in Figure 4 of the conceptual model, Ushahidi, Sahana, and Open Street Map provide a mechanism to gather, store, and display information generated socially. Receipt of that information can come from any device with SMS capability. The widespread availability of cell phones enables interested, helpful parties to quickly provide information to responders, thus closing the information gap. This was the case in Haiti (Hester, Shaw and Biewald 2010).

Areas to investigate in using the crowd sourcing technique include vetting, standardization in messaging, and the required level of trust, or security, in the portal (Chlebo, Christman and Johnson 2011). These should not be seen as reasons not to crowdsource, but as challenges to address, because the effectiveness of crowd sourcing has been demonstrated. For example, crowdsourced reports saved lives during the Haitian earthquake response (McKenna 2010).

The key to taking advantage of crowd source information lies in well-defined conditions for use, such as the following five proposed by Euchner (2010):

> 1) The problem (and its boundary conditions) must be well defined; 2) The population of potential solvers with relevant expertise must be large, 3) Feedback must be provided to the crowd (not just to individual contributors) so that ideas can evolve, 4) Mechanisms for managing intellectual property must be in place, and 5) Someone needs to filter the ideas (and develop them).

When these conditions are met, crowdsourced information may have significant value.

III. ANALYSIS OF VARIOUS INFORMATION-SHARING EFFORTS

A. CHALLENGES FOR SHARING INFORMATION

1. Usability or Security

There are tradeoffs to make in the areas of security and usability. The most stringent security measures would result in a classified system only usable by cleared personnel. Since Koinonia is designed to enable information sharing between a wide set of potential collaborators, including those who lack clearance, such measures would not be appropriate. There are other security measures that should be employed to enhance information assurance on unclassified systems.

2. Interoperability as a Requirement

EUCOM's Combined Endeavor exercise involves rigorous tests of multinational communications systems. One of the findings of those tests is that network interoperability can be made challenging by national policies (Gateau 2012). Some nations require the exclusion of foreign network administrators from their national intranet, blocking access at their router. Other nations will permit their allies to manage network traffic up to their firewall, and will then permit visibility but not control one level beyond that firewall. A federated management approach, which permits network administrators of cooperating nations to ensure the compliance of their networks with the overall requirements, has been successful. Taking such an approach with Koinonia would result in organizations retaining control of their own hardware and configurations, but has the drawback of potentially depending on administrators with less capable tools, or skill, to enforce the compliance of their portion of the network with security and interoperability standards. One method of mitigating that risk without asking nations or organizations to surrender control of their networks is to provide them with liaisons that do not control their network, but whom they permit to view its configuration and observe its compliance. Granting such a liaison permission to monitor but not alter network configuration may be a useful method of ensuring trust between information-sharing partners.

3. Transition to Their Fight: After U.S. Withdrawal

The withdrawal of U.S. forces from an area of operations potentially creates a void in capabilities in a variety of areas, such as combat power, logistics, and manpower, among others. The loss of capability in these areas can be mitigated by foreign weapon sales, use of local resources, and training of local personnel. The greatest loss may come from the withdrawal of the networks and U.S.-owned information-sharing platforms.

A sudden void in the collection, management, and exploitation of data is difficult for any country to fill, particularly for those already facing resource constraints. For missions where U.S. involvement is likely to terminate before the mission's conclusion, partner nations need a platform which they may rely upon from the beginning of the engagement, and which they have a reasonable expectation of keeping and maintaining after the departure of U.S. forces.

B. EXAMINATION OF POTENTIAL SOLUTIONS

In an effort to find potential solutions, we will look at systems already in place, systems under development, and pieces of technology key to connecting the systems. We will conclude this examination by analyzing the shortfalls of these systems to identify the requirements of Koinonia.

1. APAN: All Partners Access Network

The All Partners Access Network, formerly the Asia-Pacific Area Network, was created by PACOM to use public domain materials and web-based technology to support PACOM's security cooperation initiatives. The portal went live in March of 2000 and was used primarily for Humanitarian Assistance / Disaster Relief missions, partnership building, and joint exercises.

a. Examine APAN as Data Sharing Model

APAN serves as a collection of hosted files, with associated tools, accessible with a username and password through a web portal. It cannot stream live data. Files need to be complete in order to be uploaded and hosted, so a video of something taking place in real time could not be shared, because the file is still being created. Once the file is saved and is not being written it can be uploaded to APAN, but a live VTC (Video Teleconference) or live stream from a security camera could not be shared across APAN.

b. Limitations of APAN

(1) Cannot do tactical ISR feeds. APAN has a limitation in that the maximum file size that can be uploaded to the portal is 100MB. That size limitation does not permit for high-resolution video of any significant duration. (For reference, 150MB per minute is a typical size requirement for a resolution of 1080p, although this will vary by compression method and subject matter.)

(2) No real-time sharing on the portal. APAN does not support live streams, whether of video or audio. Uploads to the portal consist of completed files, not files that are currently being written.

(3) Human in the loop: must go looking for data. APAN does support communities of interest, so that a user can sign up for only relevant communities in an effort to avoid being inundated with information that is not of interest to him. This still means that a user will need to log in to APAN frequently and look for recently uploaded information if his work requires near real-time collaboration.

(4) Use of APAN creates a functional dependency on U.S. networks. APAN is a DISA product, and its servers are military property. This is not necessarily a problem, but it is a theoretical possibility that if U.S. or DoD involvement in a particular mission or area ended or became unfunded, that the network resources could be reallocated to other tasks, leaving former partners in the lurch. Using U.S.

military servers as the sole central repository for all data may not be universally desirable.

2. CWIX: Coalition Warrior Interoperability eXploration, eXperimentation and eXamination

> The Coalition Warrior Interoperability eXploration, eXperimentation and eXamination eXercise (CWIX) programme provides an opportunity for NATO Nations, Partner Nations, Contact Nations, and NATO Agencies to prove, disprove, and improve NATO CIS interoperability.
>
> CWIX is a major initiative to test, assess, and improve the interoperability of NATO and national CIS systems with particular emphasis on those that would be deployed with NATO-led operations such as ISAF, Active Endeavour, KFOR and Operation Ocean Shield or within a NATO Response Force (NRF). CWIX 2013 is focused on addressing specific command and control issues in ISAF and the future mission network (FMN). (NATO 2013)

3. Commercial Applications

a. TARGETR

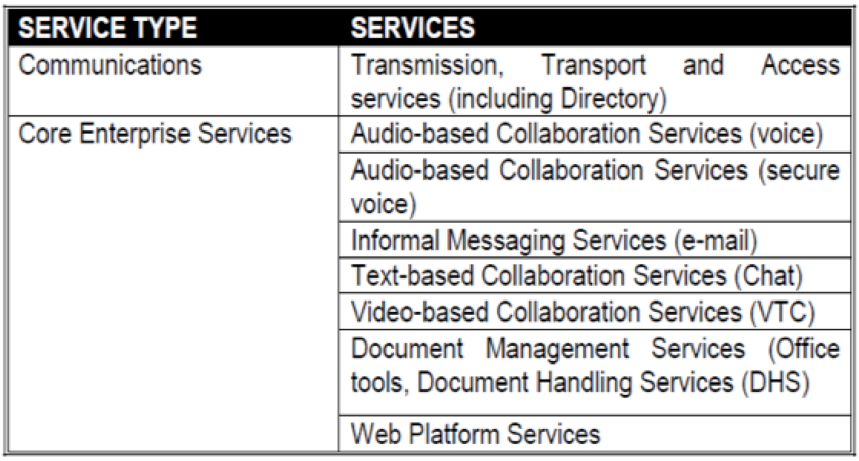
An example of commercially available unclassified intelligence innovation, Atlascraft has developed a product called Targetr to draw upon and fuse large sets of unclassified data to create powerful intelligence products and predictive capabilities. Targetr examines the relationships between data sets and attributes that include vessel AIS data, port records, names, and business contact information to detect anomalies and threats and identifies discrepancies between predicted and detected behavior. This data can be gathered from publically available internet sources, or purchased, as from a vendor such as Orbcomm or ExactEarth, both of which own satellites which collect AIS (Automatic Identification System) transmissions from shipping. Targetr is able to display the results of its fusion processes, including tracking information on a vector-based map, such as the geographic information systems developed by NASA or Google.

4. Current Collaborative Networks

There are several existing networks that address information-sharing needs that have similar, but not identical, requirements to that of Koinonia. These networks are large, permanent, and are capable of handling classified data.

a. FMN: Future Mission Network

FMN is designed to permit hasty network setup for coalition missions, enable releasable Secret communications between multinational military units in no more time than it would take to establish national networks like SIPRNet or NIPRNet. They are colloquially referred to as “Human to Human” communication services (Leca 2012). The list of these core services is shown in Table 2.



SERVICE TYPE	SERVICES
Communications	Transmission, Transport and Access services (including Directory)
Core Enterprise Services	Audio-based Collaboration Services (voice)
	Audio-based Collaboration Services (secure voice)
	Informal Messaging Services (e-mail)
	Text-based Collaboration Services (Chat)
	Video-based Collaboration Services (VTC)
	Document Management Services (Office tools, Document Handling Services (DHS)
	Web Platform Services

Table 2. “Human to Human” communication services (From Leca 2012).

The goal of quick setup is one which it would share with the hypothetical Koinonia network, but the more robust capability that FMN delivers in enabling classified communication would necessarily limit the potential partners with whom U.S. military units could connect. There may nations with whom the U.S. might work on a FID (Foreign Internal Defense) mission, or a HA/DR mission, but with whom the U.S. cannot share Secret data. This restriction on which organizations FMN could make into potential information-sharing partners also applies to NGOs, which can only communicate at the unclassified level.

NATO has a draft FMN profile that will be tested against the U.S. Mission Partner Environment (MPE) profile in NATO's 2013 CWIX exercise at the Joint Force Training Centre (JFTC), in Bydgoszcz, Poland. The testing areas and partners are outlined in Table 3 below. The U.S. MPE has previously gone by the name of FMN, which in turn developed from the Afghanistan Mission Network (AMN).

SITE	NETWORK	Core Enterprise Services					CD Cap	
Core Enterprise Services Assessment - Execution Weeks	**Event Network**	E-Mail Routing Service (ERS)	Voice over Internet Protocol (VoIP)	Chat	Web Browsing Services (WBS)	Document Handling Services (DHS)	CD-Chat	CD-Voice
Canada (CAN)	CTE2	**X**	**X**	**X**	**X**	**X**	**X**	
DENMARK (DEN)	CWIX			**X**				
C4AD - Suffolk	CTE2	**X**	**X**	**X**	**X**	**X**	**X**	**X**
NETHERLANDS (NLD)	CWIX	**X**	**X**	**X**	**X**	**X**	**X**	
FRANCE (FRA)	CTE2			**X**				
FINLAND (FIN) Distributed	CWIX	**X**		**X**	**X**	**X**		
NATO JWC	CWIX	**X**	**X**	**X**	**X**	**X**		
NCIA - IETV	CWIX			**X**			**X**	**X**
NCIA - Mons	CTE2	**X**	**X**	**X**	**X**	**X**		
NCIA - T Hague	CTE2		**X**	**X**	**X**	**X**	**X**	
USA - JITC- IH	CTE2	**X**		**X**			**X**	**X**
USA - CTSF	CTE2	**X**	**X**	**X**	**X**	**X**	**X**	**X**
USA - NATEX - Mons	CTE2	**X**	**X**	**X**	**X**	**X**	**X**	**X**
SWE - Bydg	CWIX	**X**		**X**	**X**	**X**		
SWE - Enkoping	CTE2	**X**	**X**	**X**	**X**	**X**	**X**	
GBR - Blandford	CTE2	**X**	**X**	**X**	**X**	**X**		
GBR (MET) TBD								
USA - C4AD - Bdyg	CWIX	**X**	**X**	**X**	**X**	**X**	**X**	**X**
ITA - Bydg	CWIX	**X**	**X**	**X**	**X**	**X**	**X**	

Table 3. FMN testing areas and participants (From Allied Command Transformation Command & Control Deployability & Sustainability 2013).

b. CENTRIX: Combined Enterprise Regional Information Exchange System

CENTRIX is perhaps the most important information exchange system linking coalition military partners to U.S. forces. It permits the exchange of up to Secret Releasable information between participating nations. NGOs do not have access. There are lots of separate networks with specific purposes and clearly defined users, including bilateral agreements between the U.S. and one other nation, regional enclaves with several participating nations, and mission-specific enclaves where national participation may change over time. These various networks do not communicate, and must be entirely separate, even when the same countries have access to the same CENTRIX enclaves. This may necessitate a U.S. military unit running several different instances of CENTRIX and communicating with different nations about the same event on each, with no ability to "forward," "copy," or "paste" data between them. Making a real-time report to all coalition partners in an area with such overlap can mean literally typing the same words into three or more different laptops so that military partners from three or more different nations are informed.

c. GCTF: Global Counter-Terrorism Task Force

This is one of the CENTRIX enclaves, used in CENTCOM by naval forces working near the Horn of Africa or in the Arabian Gulf. CENTRIX-GCTF was also used in Afghanistan, where as many as 66 different nations participated in Operation Enduring Freedom.

d. BICES: Battlefield Information Collection & Exploitation System

A powerful new model network for sharing information at a classified level, BICES suffers from an information gap, meaning that information does not go directly to it natively, but is transferred to it from the national classified networks of some two dozen NATO nations. Some of this gap between what is available on SIPRNet, for example, and on BICES may be attributed the relative immaturity of the network, which has had only a few years of operational life in which to amass data from collections. (BICES and SIPRNet are capable of processing information of the same level of classification.) A second problem stems from the lack of trust in the new network. Familiarity with the system is increasing and more NATO countries are using the network, so more material is being gathered. However, the greatest obstacle still exists for BICES; namely, the lack of dedicated feeds into the system. Countries collect material on national systems, authorized it for disclosure, and then transfer it to BICES. In order to be a successful information collection and exploitation platform, BICES would require direct feeds, but it is not intended to fill that role and was designed as a connection between national networks. The desirability of direct feeds will be true for Koinonia as well, especially since it would be even harder to transfer even releasable information from a classified domain such as SIPRNet to an unclassified domain.

5. Mobile Communications

A network designed to quickly support collaboration with a wide range of partners in various environments needs to be deployable, rapidly configurable, scalable, and rugged. Since mobile 3G technologies such as GSM (Global System for Mobile) are so prevalent, a network that can incorporate its use will greatly expand the number of devices and users that can reach it. For example, if a network employed during a HA/DR effort is able to accept an MMS containing an image of an urgent need and metadata containing a geotag from a local policeman, then the number of local information reporters can be quickly expanded. In addition to local users, 3G mobile technology is also typically available to aid volunteers, NGO workers, and most potential partners.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. DATA AND PROCESS ANALYSIS

After background research and literature review, we analyzed the difficulties inherent in sharing information to coalition partners across classification domains. To do this, we relied on an ongoing series of experiments that involved information gathering with coalition partners. One such experiment was conducted June 6–14, 2012. This was Tactical Networking Testbed (TNT) Maritime Interdiction Operations (MIO) experiment entitled *Networking And Interagency Collaboration On Small Craft Maritime Source Nuclear Radiological Threat Detection And Interdiction.* The overall TNT series, and this particular batch of experiments, directly apply toward sharing coalition information. They address the who, what, and how information gets shared in a multinational and multi-organizational environment, and so the lessons learned from the exercise are relevant to identifying ideal processes and tools for maximum efficiency in sharing information.

The record of these experiments come from a test database for the NATO Coaltion Warrior Interoperability eXploration, eXperimentation, eXamination, eXercise (CWIX). CIWX provides nations, agencies, commands and partners a stable, multi-domain, secure C4ISR testing environment (Allied Command Transformation Command & Control Deployability & Sustainability 2013) in order to ensure member nations have the ability to:

- Continuously improve interoperability effectiveness
- Leverage the human interactions that occur especially during execution to capitalize on potential innovations

A. TNT MIO 2012.

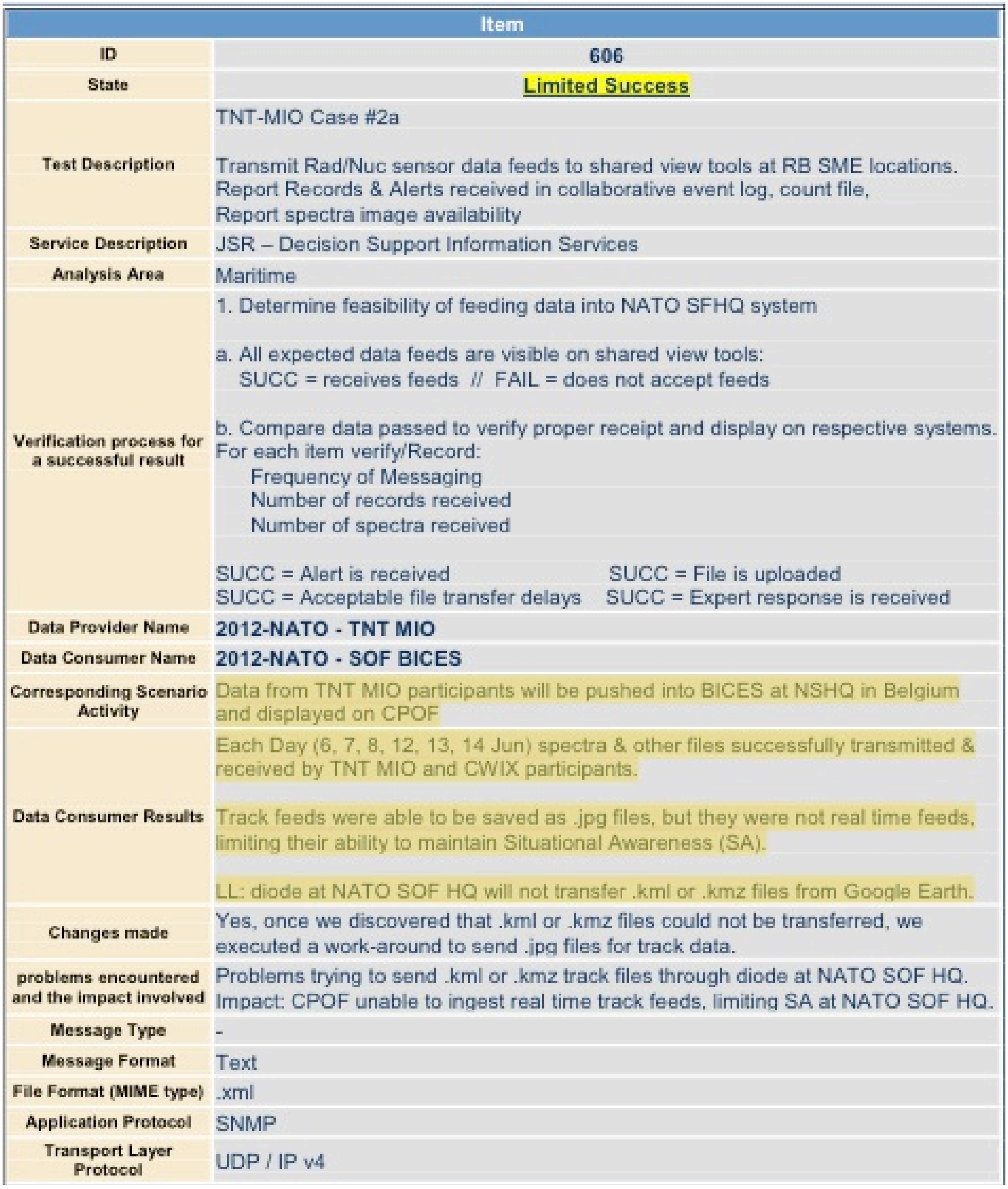
Organizations and parties represented in TNT MIO 2012 included NATO, the U.S. Defense Threat Reduction Agency (DTRA), the NATO MIO Training Center (NMIOTC), Joint Chemical, Biological, Radiological, Nuclear Defense (JCBRN) Center of Excellence (CoE), U.S. European Command (EUCOM), Norwegian Naval Special Operations Command (NORNAVSOC), and Canada SOF (NPS MDSRP, USSOCOM, DTRA 2012). This serves as a good representation of the "who" in coalition operations with parties from multiple nations, organizational types, and government agencies both military and civilian.

Together, these organizations conducted a series of MIO field experiments that included the use of networks, advanced sensors and collaborative technology to support integrated detection and interagency collaboration (Bordetsky and Netzer 2010). Disparate forces engaged in a common mission and attempted to fuse information gleaned from a variety of means with a goal of sharing and cooperating in order to conduct multilateral operations.

Finally, we examine the "how" of information sharing. Specific technology areas examined during the experiments of June 2012 include: ad hoc mobile networking architecture, information management architecture, surveillance techniques, cooperative C2 and interoperability constraints, cyber distortion, knowledge and social networking architecture, visibility and vulnerability, and capturing of models (NPS MDSRP, USSOCOM, DTRA 2012). Each of these areas either support or directly apply to coalition information sharing.

1. Situational Awareness

Arguably, one of the most important aspects of networking as applied to military operations is the situational awareness (SA) of a common operating picture (COP) created by combining sensors and reporting data. Through the use of friendly situational reports and sensor data and observations of hostile forces that are aggregated and displayed, the reviewing organizations gain an orientation to the operational area and the task at hand. To that end, information should be continuously updated in order to maximize the SA of headquarters organizations, an attempt illustrated in the example shown in Figure 6.



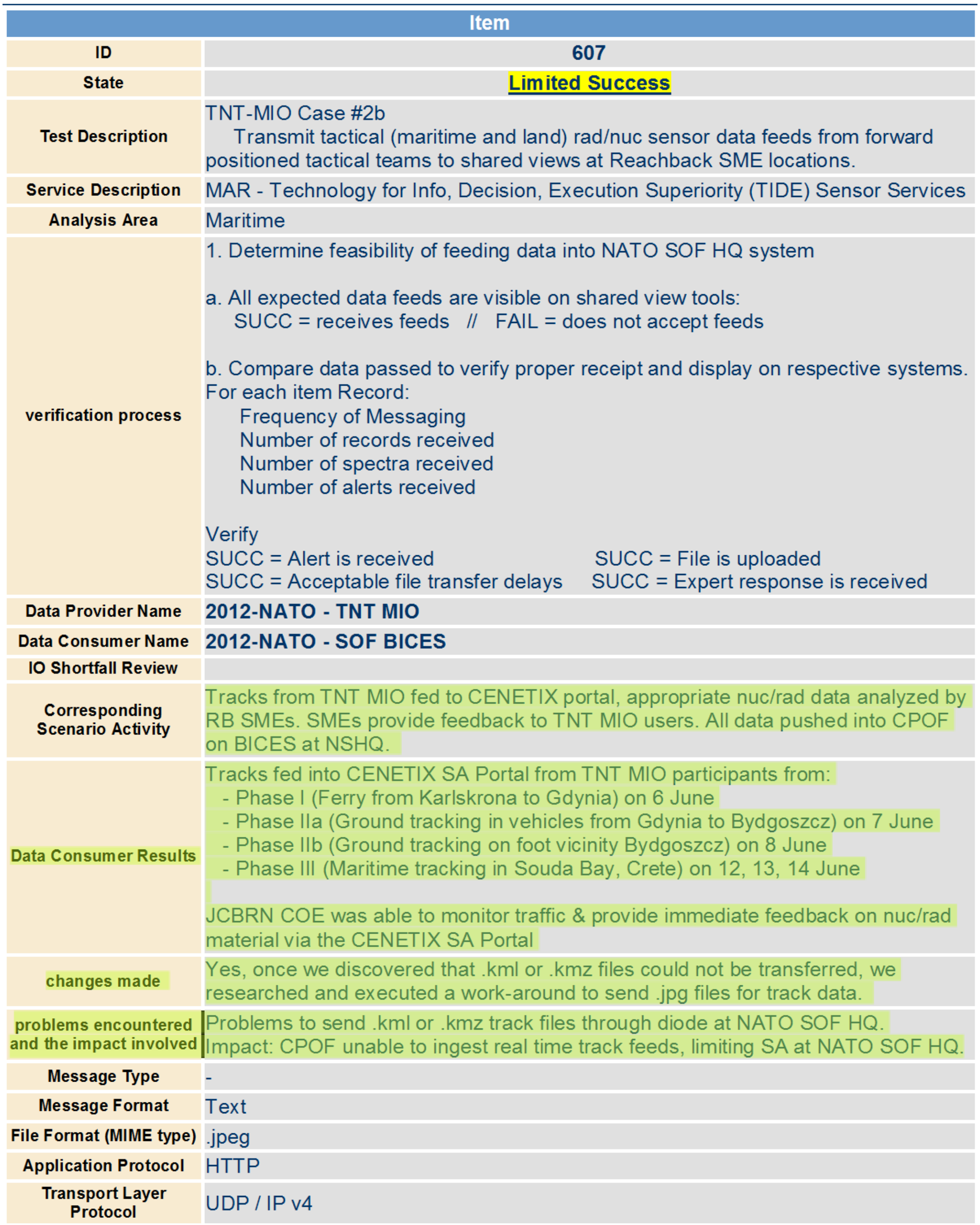
Item	
ID	606
State	Limited Success
Test Description	TNT-MIO Case #2a Transmit Rad/Nuc sensor data feeds to shared view tools at RB SME locations. Report Records & Alerts received in collaborative event log, count file, Report spectra image availability
Service Description	JSR – Decision Support Information Services
Analysis Area	Maritime
Verification process for a successful result	1. Determine feasibility of feeding data into NATO SFHQ system a. All expected data feeds are visible on shared view tools: SUCC = receives feeds // FAIL = does not accept feeds b. Compare data passed to verify proper receipt and display on respective systems. For each item verify/Record: Frequency of Messaging Number of records received Number of spectra received SUCC = Alert is received SUCC = File is uploaded SUCC = Acceptable file transfer delays SUCC = Expert response is received
Data Provider Name	**2012-NATO - TNT MIO**
Data Consumer Name	**2012-NATO - SOF BICES**
Corresponding Scenario Activity	Data from TNT MIO participants will be pushed into BICES at NSHQ in Belgium and displayed on CPOF
Data Consumer Results	Each Day (6, 7, 8, 12, 13, 14 Jun) spectra & other files successfully transmitted & received by TNT MIO and CWIX participants. Track feeds were able to be saved as .jpg files, but they were not real time feeds, limiting their ability to maintain Situational Awareness (SA). LL: diode at NATO SOF HQ will not transfer .kml or .kmz files from Google Earth.
Changes made	Yes, once we discovered that .kml or .kmz files could not be transferred, we executed a work-around to send .jpg files for track data.
problems encountered and the impact involved	Problems trying to send .kml or .kmz track files through diode at NATO SOF HQ. Impact: CPOF unable to ingest real time track feeds, limiting SA at NATO SOF HQ.
Message Type	-
Message Format	Text
File Format (MIME type)	.xml
Application Protocol	SNMP
Transport Layer Protocol	UDP / IP v4

Figure 6. Situational Awareness (From NPS MDSRP, USSOCOM, DTRA 2012)

Unfortunately, in the transfer from an unclassified system to a classified system, in this case BICES, both time and file fidelity were compromised. The combination of those losses results in a reduction of SA. When different classification levels are involved, cross domain data transfer becomes extremely challenging due to the technical properties of typical network edge devices. For successful SA to be enabled by the proposed Koinonia network, the COP ought to reside on the same classification level of the inputs. Specifically, Koinonia will avoid a host of technical problems if the network is kept at an unclassified level.

2. Loss of Functionality

An inability to process standard file formats used in common applications created a loss of functionality, as shown in Figure 7. The inability to send Google Earth .kml and .kmz files to the classified network forced a conversion to .jpeg for transfer. The .jpeg images could not be used to render a live feed showing movement. Rather, they only provided a time-delayed snapshot of the situation. Additionally, .jpeg files cannot be manipulated using commonly available display tools like Google Earth or NASA's open source World Wind virtual globe.



Item	
ID	607
State	Limited Success
Test Description	TNT-MIO Case #2b Transmit tactical (maritime and land) rad/nuc sensor data feeds from forward positioned tactical teams to shared views at Reachback SME locations.
Service Description	MAR - Technology for Info, Decision, Execution Superiority (TIDE) Sensor Services
Analysis Area	Maritime

verification process	1. Determine feasibility of feeding data into NATO SOF HQ system
	a. All expected data feeds are visible on shared view tools:
	SUCC = receives feeds // FAIL = does not accept feeds
	b. Compare data passed to verify proper receipt and display on respective systems. For each item Record:
	Frequency of Messaging
	Number of records received
	Number of spectra received
	Number of alerts received
	Verify
	SUCC = Alert is received SUCC = File is uploaded
	SUCC = Acceptable file transfer delays SUCC = Expert response is received

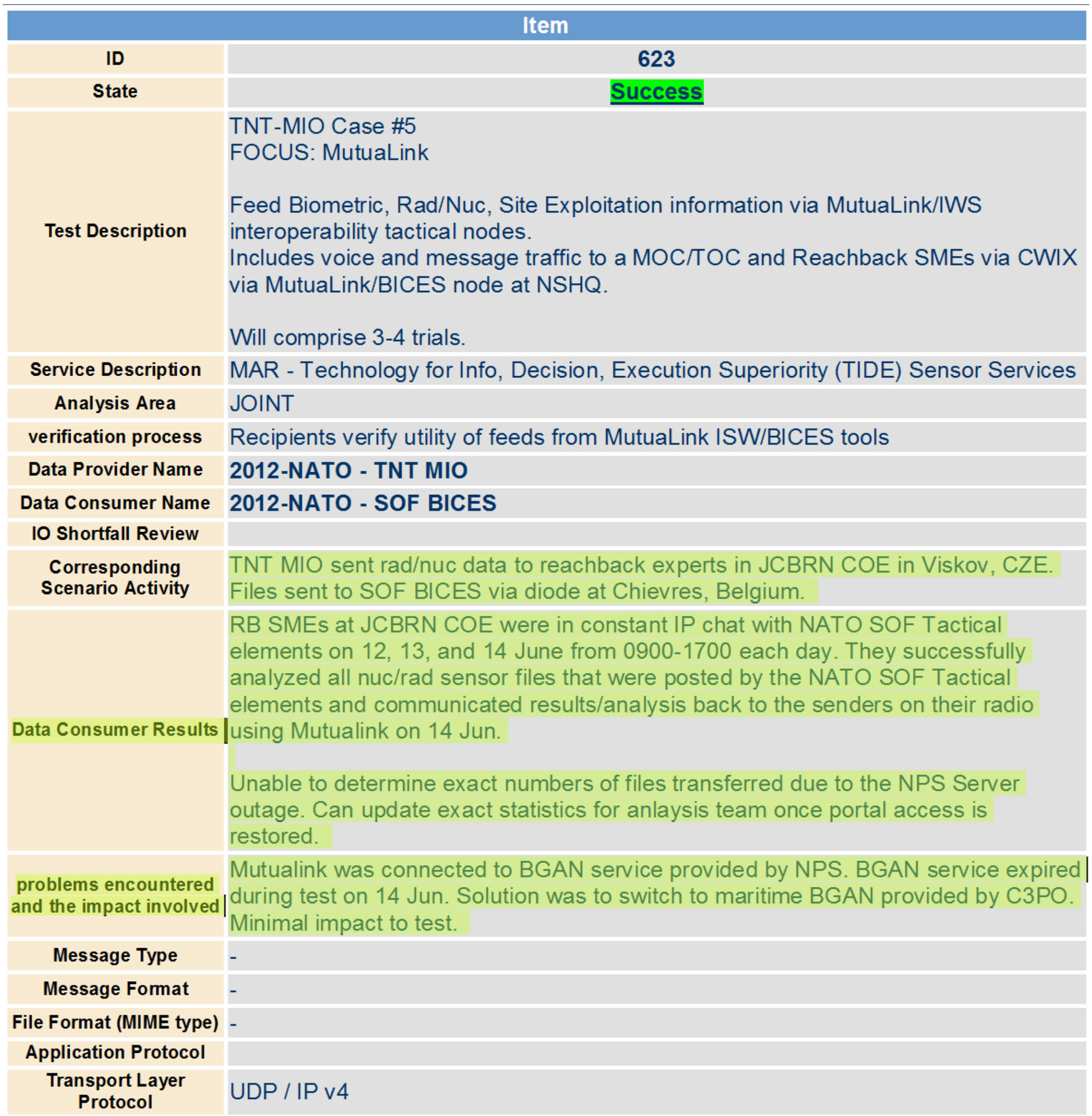
Data Provider Name	**2012-NATO - TNT MIO**
Data Consumer Name	**2012-NATO - SOF BICES**
IO Shortfall Review	
Corresponding Scenario Activity	Tracks from TNT MIO fed to CENETIX portal, appropriate nuc/rad data analyzed by RB SMEs. SMEs provide feedback to TNT MIO users. All data pushed into CPOF on BICES at NSHQ.
Data Consumer Results	Tracks fed into CENETIX SA Portal from TNT MIO participants from: - Phase I (Ferry from Karlskrona to Gdynia) on 6 June - Phase IIa (Ground tracking in vehicles from Gdynia to Bydgoszcz) on 7 June - Phase IIb (Ground tracking on foot vicinity Bydgoszcz) on 8 June - Phase III (Maritime tracking in Souda Bay, Crete) on 12, 13, 14 June JCBRN COE was able to monitor traffic & provide immediate feedback on nuc/rad material via the CENETIX SA Portal
changes made	Yes, once we discovered that .kml or .kmz files could not be transferred, we researched and executed a work-around to send .jpg files for track data.
problems encountered and the impact involved	Problems to send .kml or .kmz track files through diode at NATO SOF HQ. Impact: CPOF unable to ingest real time track feeds, limiting SA at NATO SOF HQ.
Message Type	-
Message Format	Text
File Format (MIME type)	.jpeg
Application Protocol	HTTP
Transport Layer Protocol	UDP / IP v4

Figure 7. Case for Functionality (From NPS MDSRP, USSOCOM, DTRA 2012)

Maintaining material on the originating network allows operators to keep file functionality. So long as Koinonia lies on the same classification level as open and crowdsourced material, it will be possible to maintain full functionality of the files as well as to maintain real time reporting.

3. Overreliance on Satellite Communications

Data paths from the mobile teams involved using low bandwidth mobile satellite services. These satellite services are subject to outages, as in Figure 8. Outages can occur for a variety of reasons including lease limitations, weather, and equipment issues. Also, they required the unit to stop moving, set up the antenna, and then conduct communications. Further, the cost for satellite time is high, so that usage must be kept to a minimum, even if the host country can afford the initial cost of the system.



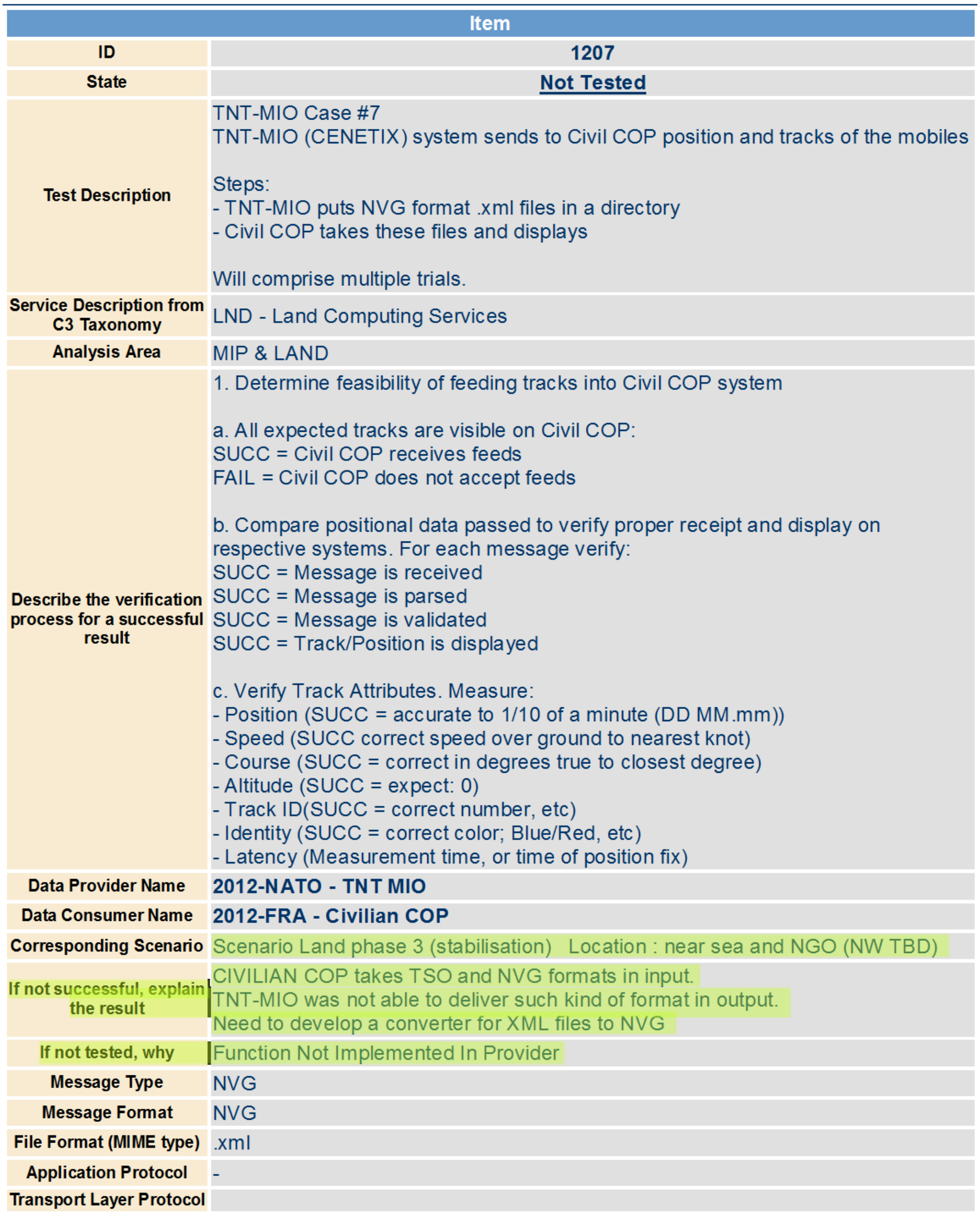
Item	
ID	623
State	Success
Test Description	TNT-MIO Case #5 FOCUS: MutuaLink Feed Biometric, Rad/Nuc, Site Exploitation information via MutuaLink/IWS interoperability tactical nodes. Includes voice and message traffic to a MOC/TOC and Reachback SMEs via CWIX via MutuaLink/BICES node at NSHQ. Will comprise 3-4 trials.
Service Description	MAR - Technology for Info, Decision, Execution Superiority (TIDE) Sensor Services
Analysis Area	JOINT
verification process	Recipients verify utility of feeds from MutuaLink ISW/BICES tools
Data Provider Name	2012-NATO - TNT MIO
Data Consumer Name	2012-NATO - SOF BICES
IO Shortfall Review	
Corresponding Scenario Activity	TNT MIO sent rad/nuc data to reachback experts in JCBRN COE in Viskov, CZE. Files sent to SOF BICES via diode at Chievres, Belgium.
Data Consumer Results	RB SMEs at JCBRN COE were in constant IP chat with NATO SOF Tactical elements on 12, 13, and 14 June from 0900-1700 each day. They successfully analyzed all nuc/rad sensor files that were posted by the NATO SOF Tactical elements and communicated results/analysis back to the senders on their radio using Mutualink on 14 Jun. Unable to determine exact numbers of files transferred due to the NPS Server outage. Can update exact statistics for anlaysis team once portal access is restored.
problems encountered and the impact involved	Mutualink was connected to BGAN service provided by NPS. BGAN service expired during test on 14 Jun. Solution was to switch to maritime BGAN provided by C3PO. Minimal impact to test.
Message Type	-
Message Format	-
File Format (MIME type)	-
Application Protocol	
Transport Layer Protocol	UDP / IP v4

Figure 8. Reliance on Satellite communications (From NPS MDSRP, USSOCOM, DTRA 2012)

Using terrestrial commercial services can obviate the need for costly or limited access satellite communications usually utilized by well-funded military forces. Providing a method for cellular communications allows for communications on-the-move and lowers cost compared to satellite communications. This also allows for other parties to participate in the information gathering. Just as data collected from cell phones was used in a Disaster Relief situation via the Ushahidi platform (Chlebo, Christman and Johnson 2011), so too could the general populace participate in information collection to accelerate populating Koinonia with data.

4. Standardizing Message Format

The experiment shows a requirement for standardized message formats. Figure 9 reveals that the TNT MIO network was unable to provide the track format required by the civilian COP. The COP required a specific file type for input, in this case TSO or NVG. The broadcast of TNT MIO tracks were not formatted for TSO or NVG and could not be converted. The requirement of a specific format made ingestion of data into the civilian COP easy for their toolset to handle, but at the cost of making it less compatible with other broadcasts. The trial did not achieve success because incompatible message formatting standards were chosen and neither the data provider nor the recipient were capable of translating alternative formats.



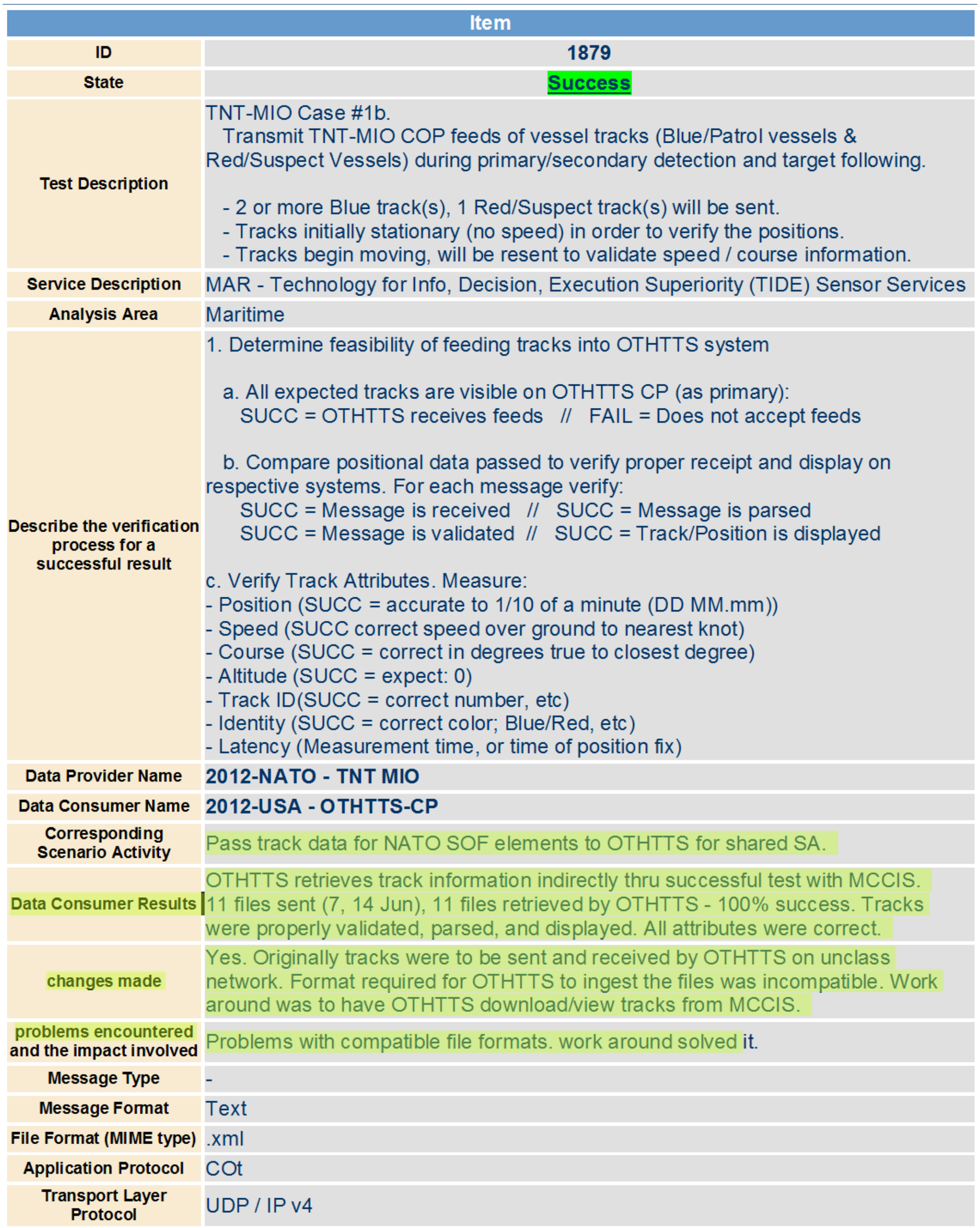
Item	
ID	1207
State	Not Tested
Test Description	TNT-MIO Case #7 TNT-MIO (CENETIX) system sends to Civil COP position and tracks of the mobiles Steps: - TNT-MIO puts NVG format .xml files in a directory - Civil COP takes these files and displays Will comprise multiple trials.
Service Description from C3 Taxonomy	LND - Land Computing Services
Analysis Area	MIP & LAND
Describe the verification process for a successful result	1. Determine feasibility of feeding tracks into Civil COP system a. All expected tracks are visible on Civil COP: SUCC = Civil COP receives feeds FAIL = Civil COP does not accept feeds b. Compare positional data passed to verify proper receipt and display on respective systems. For each message verify: SUCC = Message is received SUCC = Message is parsed SUCC = Message is validated SUCC = Track/Position is displayed c. Verify Track Attributes. Measure: - Position (SUCC = accurate to 1/10 of a minute (DD MM.mm)) - Speed (SUCC correct speed over ground to nearest knot) - Course (SUCC = correct in degrees true to closest degree) - Altitude (SUCC = expect: 0) - Track ID(SUCC = correct number, etc) - Identity (SUCC = correct color; Blue/Red, etc) - Latency (Measurement time, or time of position fix)
Data Provider Name	**2012-NATO - TNT MIO**
Data Consumer Name	**2012-FRA - Civilian COP**
Corresponding Scenario	Scenario Land phase 3 (stabilisation) Location : near sea and NGO (NW TBD)
If not successful, explain the result	CIVILIAN COP takes TSO and NVG formats in input. TNT-MIO was not able to deliver such kind of format in output. Need to develop a converter for XML files to NVG
If not tested, why	Function Not Implemented In Provider
Message Type	NVG
Message Format	NVG
File Format (MIME type)	.xml
Application Protocol	-
Transport Layer Protocol	

Figure 9. Message formatting (From NPS MDSRP, USSOCOM, DTRA 2012)

Requiring rigid messaging standardization in order to handle inputs is a double-edged sword. The tighter the requirements, the less useful the network from an outsider's perspective. The more lose the requirements, the more difficult or costly to create data paths or converters for data ingestion. Koinonia would benefit from native compatibility with the message standards of cellular data, specifically SMS and MMS. These simple messages can build a creditable picture of the operation space via tools such as the previously mentioned Ushahidi platform (Chlebo, Christman and Johnson 2011).

5. File Format Compatibility

Initially, the file format provided by TNT MIO was incompatible for entry into OTHTTS (Over The Horizon Tactical Tracking System). Outlined in Figure 10, a work around was built to have OTHTTS draw from MCCIS (Maritime Command and Control Information System), which had been successfully receiving track information. While this shows the importance of file format compatibility, it also illustrates that a robust toolset, MCCIS in this case, can mitigate shortfalls in a system.



Item	
ID	1879
State	Success
Test Description	TNT-MIO Case #1b. Transmit TNT-MIO COP feeds of vessel tracks (Blue/Patrol vessels & Red/Suspect Vessels) during primary/secondary detection and target following. - 2 or more Blue track(s), 1 Red/Suspect track(s) will be sent. - Tracks initially stationary (no speed) in order to verify the positions. - Tracks begin moving, will be resent to validate speed / course information.
Service Description	MAR - Technology for Info, Decision, Execution Superiority (TIDE) Sensor Services
Analysis Area	Maritime

Describe the verification process for a successful result	1. Determine feasibility of feeding tracks into OTHTTS system
	a. All expected tracks are visible on OTHTTS CP (as primary):
	SUCC = OTHTTS receives feeds // FAIL = Does not accept feeds
	b. Compare positional data passed to verify proper receipt and display on respective systems. For each message verify:
	SUCC = Message is received // SUCC = Message is parsed
	SUCC = Message is validated // SUCC = Track/Position is displayed
	c. Verify Track Attributes. Measure:
	- Position (SUCC = accurate to 1/10 of a minute (DD MM.mm))
	- Speed (SUCC correct speed over ground to nearest knot)
	- Course (SUCC = correct in degrees true to closest degree)
	- Altitude (SUCC = expect: 0)
	- Track ID(SUCC = correct number, etc)
	- Identity (SUCC = correct color; Blue/Red, etc)
	- Latency (Measurement time, or time of position fix)

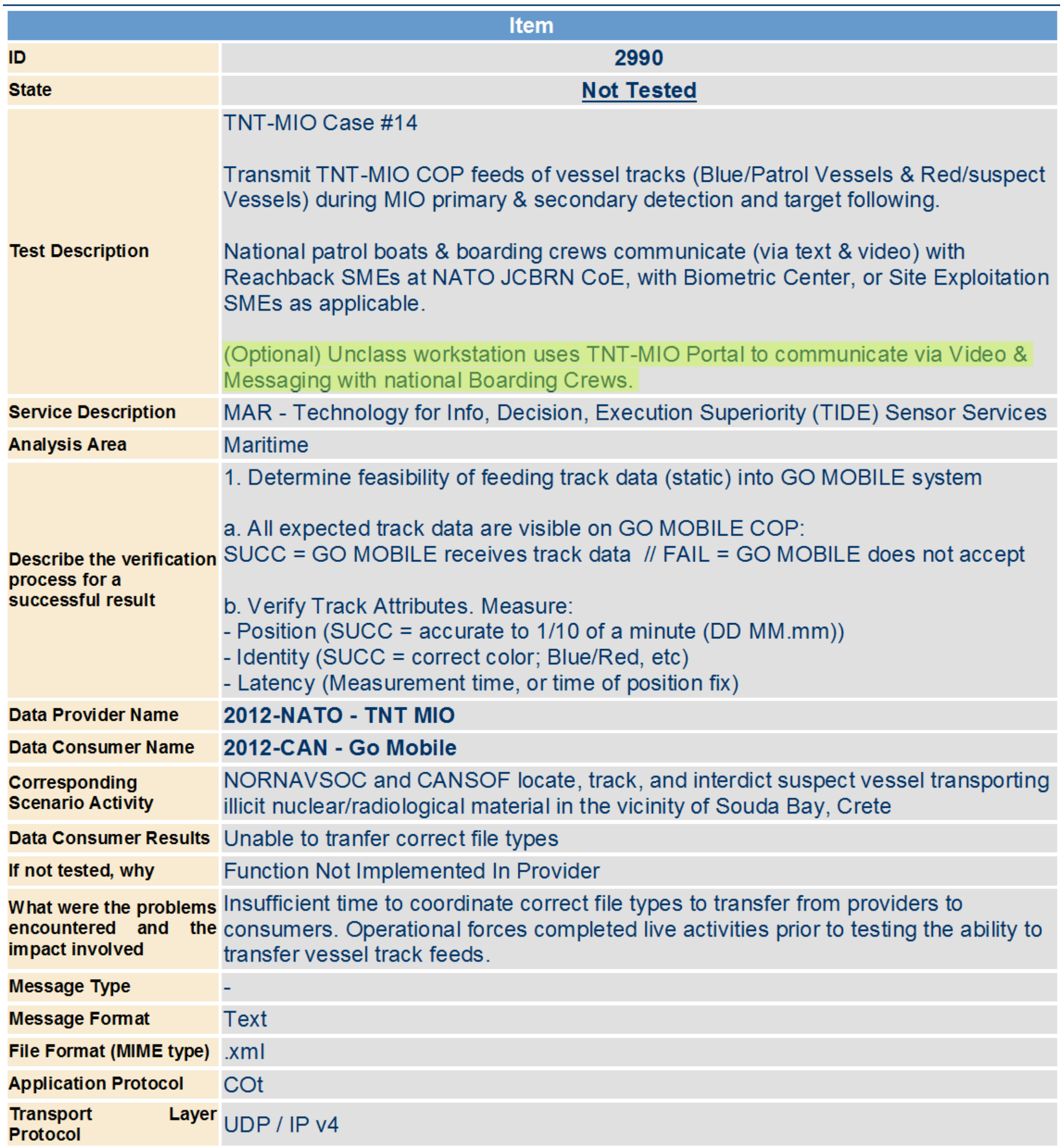
Data Provider Name	2012-NATO - TNT MIO
Data Consumer Name	2012-USA - OTHTTS-CP
Corresponding Scenario Activity	Pass track data for NATO SOF elements to OTHTTS for shared SA.
Data Consumer Results	OTHTTS retrieves track information indirectly thru successful test with MCCIS. 11 files sent (7, 14 Jun), 11 files retrieved by OTHTTS - 100% success. Tracks were properly validated, parsed, and displayed. All attributes were correct.
changes made	Yes. Originally tracks were to be sent and received by OTHTTS on unclass network. Format required for OTHTTS to ingest the files was incompatible. Work around was to have OTHTTS download/view tracks from MCCIS.
problems encountered and the impact involved	Problems with compatible file formats. work around solved it.
Message Type	-
Message Format	Text
File Format (MIME type)	.xml
Application Protocol	COt
Transport Layer Protocol	UDP / IP v4

Figure 10. File compatibility (From NPS MDSRP, USSOCOM, DTRA 2012)

Again, standardization for formatting is required. Koinonia would enjoy some advantage in a relatively limited scope for open source data. These include webpages, blogs, social media sites, as well as the discussed inputs from Ushahidi. A common element for all of these is the extensive use of XML readable feeds. Thus XML-based routing for inputs could be a powerful tool in the Koinonia network.

6. Standardizing the Network

Unclassified workstations were used to communicate with the operational elements, shown in Figure 11. Receipt of all traffic was easily accomplished at this level of classification. Most difficulties arose from the cross-domain transfer of data to a higher level of classification.



Item	
ID	**2990**
State	**Not Tested**
Test Description	TNT-MIO Case #14 Transmit TNT-MIO COP feeds of vessel tracks (Blue/Patrol Vessels & Red/suspect Vessels) during MIO primary & secondary detection and target following. National patrol boats & boarding crews communicate (via text & video) with Reachback SMEs at NATO JCBRN CoE, with Biometric Center, or Site Exploitation SMEs as applicable. (Optional) Unclass workstation uses TNT-MIO Portal to communicate via Video & Messaging with national Boarding Crews.
Service Description	MAR - Technology for Info, Decision, Execution Superiority (TIDE) Sensor Services
Analysis Area	Maritime

Describe the verification process for a successful result	1. Determine feasibility of feeding track data (static) into GO MOBILE system
	a. All expected track data are visible on GO MOBILE COP:
	SUCC = GO MOBILE receives track data // FAIL = GO MOBILE does not accept
	b. Verify Track Attributes. Measure:
	- Position (SUCC = accurate to 1/10 of a minute (DD MM.mm))
	- Identity (SUCC = correct color; Blue/Red, etc)
	- Latency (Measurement time, or time of position fix)

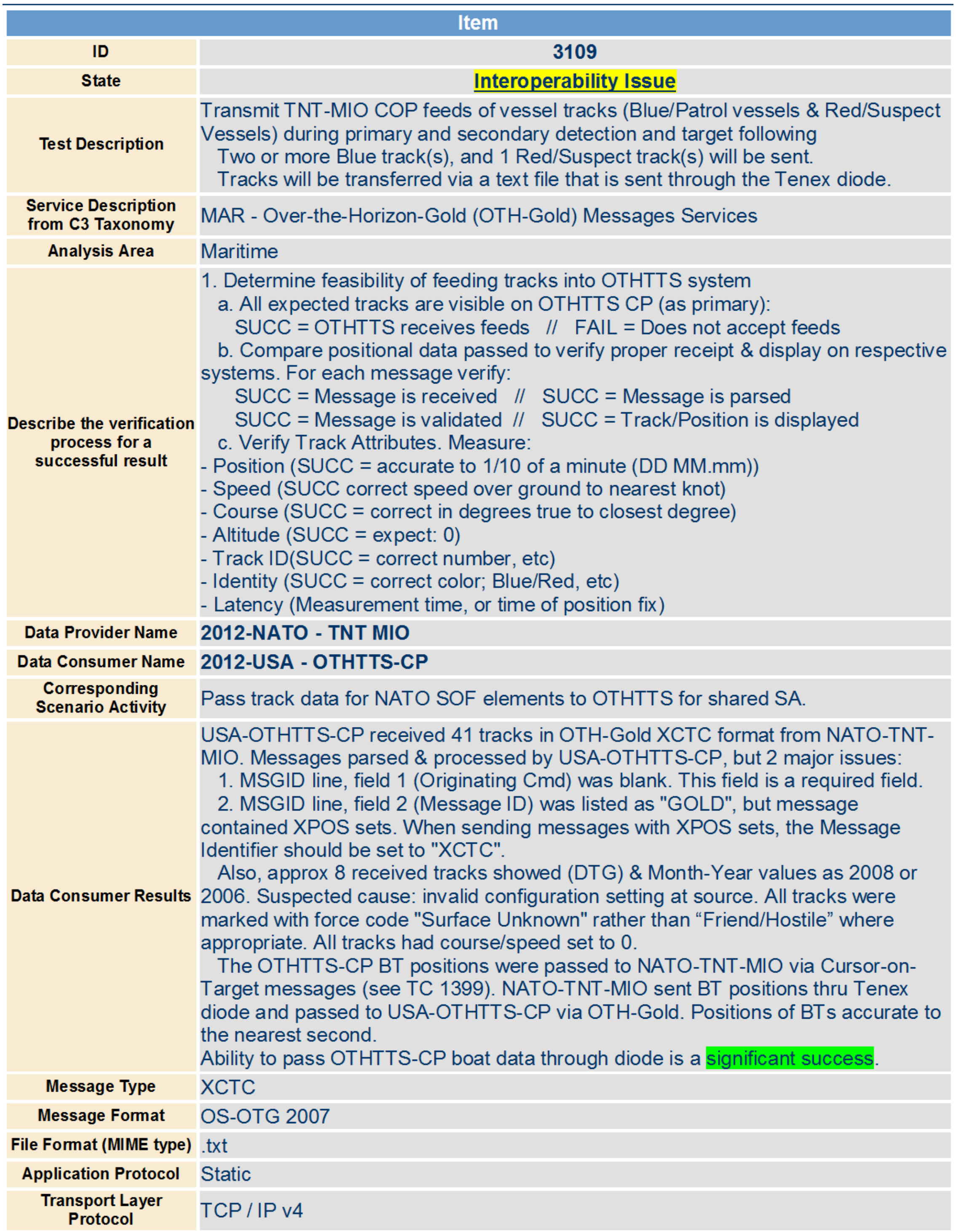
Data Provider Name	**2012-NATO - TNT MIO**
Data Consumer Name	**2012-CAN - Go Mobile**
Corresponding Scenario Activity	NORNAVSOC and CANSOF locate, track, and interdict suspect vessel transporting illicit nuclear/radiological material in the vicinity of Souda Bay, Crete
Data Consumer Results	Unable to tranfer correct file types
If not tested, why	Function Not Implemented In Provider
What were the problems encountered and the impact involved	Insufficient time to coordinate correct file types to transfer from providers to consumers. Operational forces completed live activities prior to testing the ability to transfer vessel track feeds.
Message Type	-
Message Format	Text
File Format (MIME type)	.xml
Application Protocol	COt
Transport Layer Protocol	UDP / IP v4

Figure 11. Network standardization (From NPS MDSRP, USSOCOM, DTRA 2012)

While not explicitly tested, testers identified the need to maintain data on a network accessible by all forces. This can be accomplished by maintaining and working with the data at the original level of classification. As Koinonia would be drawing from unclassified open source material, it should maintain that level of classification for the network, permitting availability to all parties and use with all openly available toolsets.

7. Interoperability

In the test describes in Figure 12, messages were successfully passed over two systems by creating a workaround which translated one message format into another. A robust toolset capable of interpreting multiple alternative formats is a powerful resource in coalition operations since it can be used as an interpreter between two other systems which would otherwise be unable to communicate. In the test described below, Cursor-on-Target (COT) messages had to be translated into Over-the-Horizon-(OTH) Gold format, and the conversion was imperfect but possible.



Item	
ID	3109
State	Interoperability Issue
Test Description	Transmit TNT-MIO COP feeds of vessel tracks (Blue/Patrol vessels & Red/Suspect Vessels) during primary and secondary detection and target following Two or more Blue track(s), and 1 Red/Suspect track(s) will be sent. Tracks will be transferred via a text file that is sent through the Tenex diode.
Service Description from C3 Taxonomy	MAR - Over-the-Horizon-Gold (OTH-Gold) Messages Services
Analysis Area	Maritime

Describe the verification process for a successful result	1. Determine feasibility of feeding tracks into OTHTTS system
	a. All expected tracks are visible on OTHTTS CP (as primary):
	SUCC = OTHTTS receives feeds // FAIL = Does not accept feeds
	b. Compare positional data passed to verify proper receipt & display on respective systems. For each message verify:
	SUCC = Message is received // SUCC = Message is parsed
	SUCC = Message is validated // SUCC = Track/Position is displayed
	c. Verify Track Attributes. Measure:
	- Position (SUCC = accurate to 1/10 of a minute (DD MM.mm))
	- Speed (SUCC correct speed over ground to nearest knot)
	- Course (SUCC = correct in degrees true to closest degree)
	- Altitude (SUCC = expect: 0)
	- Track ID(SUCC = correct number, etc)
	- Identity (SUCC = correct color; Blue/Red, etc)
	- Latency (Measurement time, or time of position fix)

Data Provider Name	2012-NATO - TNT MIO
Data Consumer Name	2012-USA - OTHTTS-CP
Corresponding Scenario Activity	Pass track data for NATO SOF elements to OTHTTS for shared SA.
Data Consumer Results	USA-OTHTTS-CP received 41 tracks in OTH-Gold XCTC format from NATO-TNT-MIO. Messages parsed & processed by USA-OTHTTS-CP, but 2 major issues: 1. MSGID line, field 1 (Originating Cmd) was blank. This field is a required field. 2. MSGID line, field 2 (Message ID) was listed as "GOLD", but message contained XPOS sets. When sending messages with XPOS sets, the Message Identifier should be set to "XCTC". Also, approx 8 received tracks showed (DTG) & Month-Year values as 2008 or 2006. Suspected cause: invalid configuration setting at source. All tracks were marked with force code "Surface Unknown" rather than "Friend/Hostile" where appropriate. All tracks had course/speed set to 0. The OTHTTS-CP BT positions were passed to NATO-TNT-MIO via Cursor-on-Target messages (see TC 1399). NATO-TNT-MIO sent BT positions thru Tenex diode and passed to USA-OTHTTS-CP via OTH-Gold. Positions of BTs accurate to the nearest second. Ability to pass OTHTTS-CP boat data through diode is a significant success.
Message Type	XCTC
Message Format	OS-OTG 2007
File Format (MIME type)	.txt
Application Protocol	Static
Transport Layer Protocol	TCP / IP v4

Figure 12. Interoperability (From NPS MDSRP, USSOCOM, DTRA 2012)

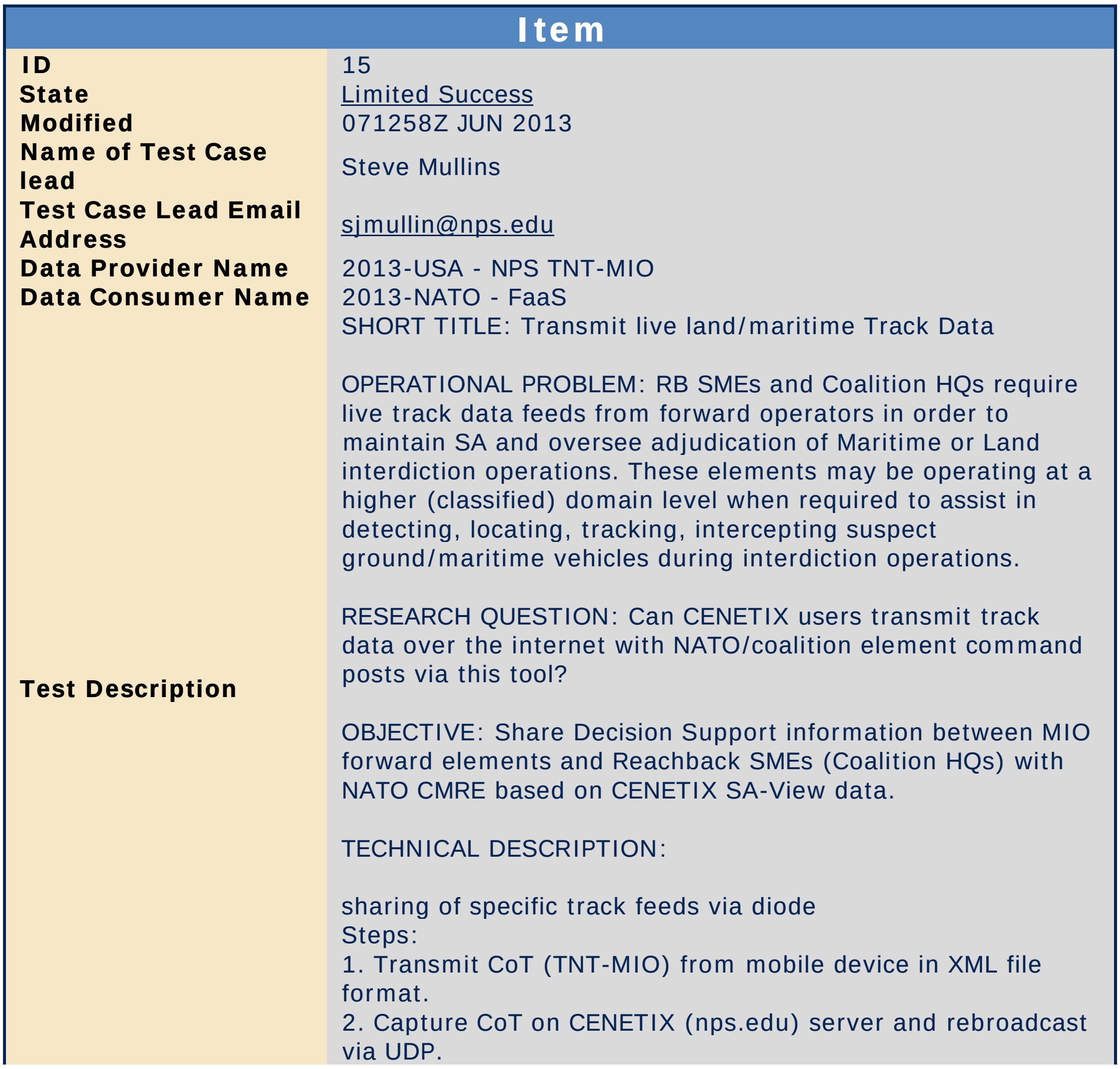
The workarounds created for the test proved effective, but the key to success will be adhering to a standard from the beginning of a program in order to minimize conversion middleware in a system. Minimization of such middleware will lower overall costs and barriers to interoperability, resulting in a system more accessible to all parties. The lesson for Koinonia it that it must be compatible with the standards of partner organizations, while keeping requirements and system cost manageable.

B. TNT MIO 2013

A follow on series of experiments was set up for 2013. Performed and reported during CWIX 2013, days prior to this documents submission for publication, two reports are instructive regarding sharing information with coalition partners.

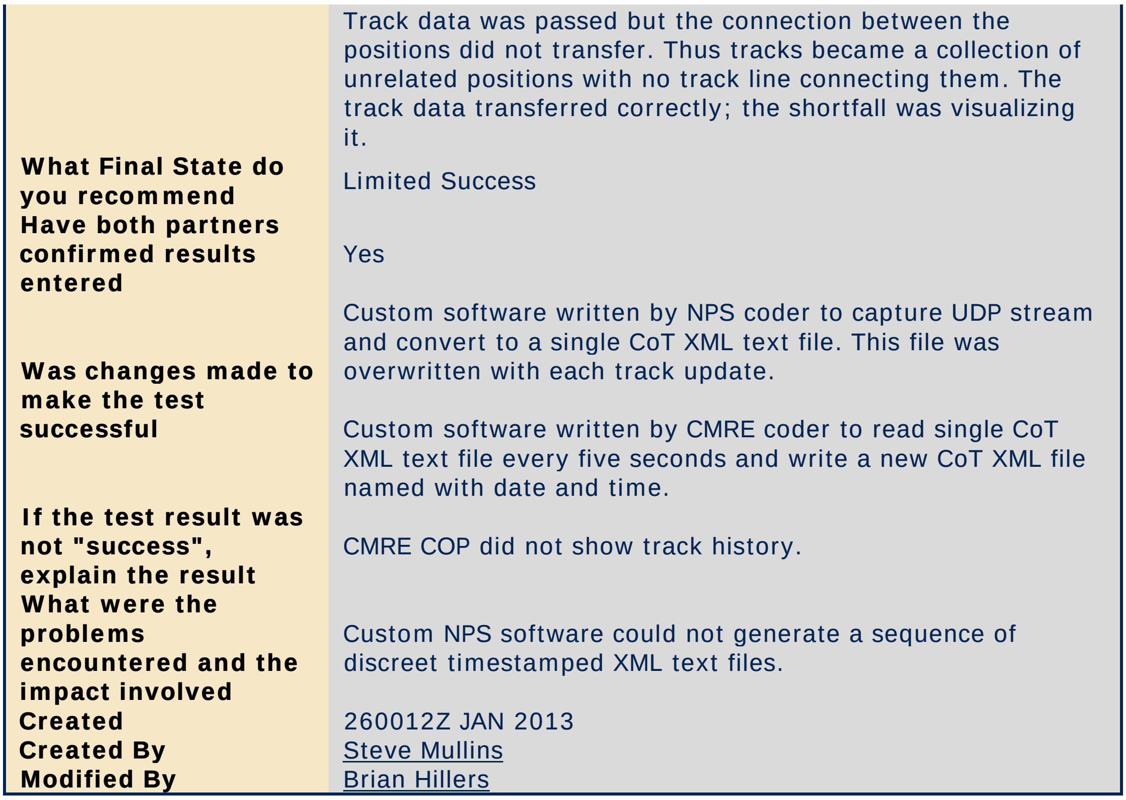
1. Pushing Track Data

Test 15 was resolved and provides a good indication for the rest of the battery of tests. The test description, results and conditions can be found in Figure 13.



Item	
ID	15
State	Limited Success
Modified	071258Z JUN 2013
Name of Test Case lead	Steve Mullins
Test Case Lead Email Address	sjmullin@nps.edu
Data Provider Name	2013-USA - NPS TNT-MIO
Data Consumer Name	2013-NATO - FaaS
Test Description	SHORT TITLE: Transmit live land/maritime Track Data OPERATIONAL PROBLEM: RB SMEs and Coalition HQs require live track data feeds from forward operators in order to maintain SA and oversee adjudication of Maritime or Land interdiction operations. These elements may be operating at a higher (classified) domain level when required to assist in detecting, locating, tracking, intercepting suspect ground/maritime vehicles during interdiction operations. RESEARCH QUESTION: Can CENETIX users transmit track data over the internet with NATO/coalition element command posts via this tool? OBJECTIVE: Share Decision Support information between MIO forward elements and Reachback SMEs (Coalition HQs) with NATO CMRE based on CENETIX SA-View data. TECHNICAL DESCRIPTION: sharing of specific track feeds via diode Steps: 1. Transmit CoT (TNT-MIO) from mobile device in XML file format. 2. Capture CoT on CENETIX (nps.edu) server and rebroadcast via UDP.

Describe the verification process for a successful result	3. Receive CoT (TNT-MIO) XML track from an external TNT-MIO portal, through diode. 4. Capture UDP stream into text files stored on CWIX low side folder. 5. Use diode to push text file from CWIX low to high. 6. Import XML track files into tracking software. POC at CMRE: Steve Horn a. CRITERIA. For each message, Report: - Receipt (SUCC = Message is received {1,0}) - Parsing (SUCC = Message is parsed {1,0}) - Valid (SUCC = Message is validated {1,0}) - Display (SUCC = Track/Position is displayed) T = {P, S, C, Alt, Trk-ID, IconID, Lat} b. CONSTRAINTS. - Single IP source c. INTEGRATION VARIABLES. Report: - Position (SUCC = accurate to 1/10 minute) - Speed (SUCC correct speed to nearest knot) - Course (SUCC = correct in degrees true to closest degree) (optional) - Altitude (SUCC = expect: 0 for maritime) (optional) - Track ID (SUCC = correct number, etc) - Identity (SUCC = correct Icon color; Blue/Red, etc) - Latency (Measurement time, or time of position fix)
Service description from C3 Taxonomy	MAR - Technology for Information, Decision and Execution Superiority (TIDE) Sensor Services
Which "X" best describes this test case	eXperimentation
Date(s) test will be executed	06 June 2013
Time(s) test case will be executed	1000Z
Estimated time it will take to complete the test	30 minutes
Next date test case will be retested	10 June 2013
Message Type	
Message Format	Text
File Format (MIME type)	.xml
Application Protocol	CoT
Transport Layer Protocol	UDP / IP v4
Corresponding Scenario Activity Description	Unrelated to CWIX scenario; situation based on separate NPS MIO Experiment where NATO SOF are pursuing notional rad/nuc materials smugglers in real time, across Germany and Poland. Live experimentation.
Data Consumer Result (larger field)	Specific criteria: SUCCESS for criteria 1-3 SUCCESS for Integration Variables: P, S, Track ID. C, A not sent (optional) SUCCESS regarding latency: no testbed system latency, however refresh rate was set at 3-5 seconds - which is will within acceptable parameters.



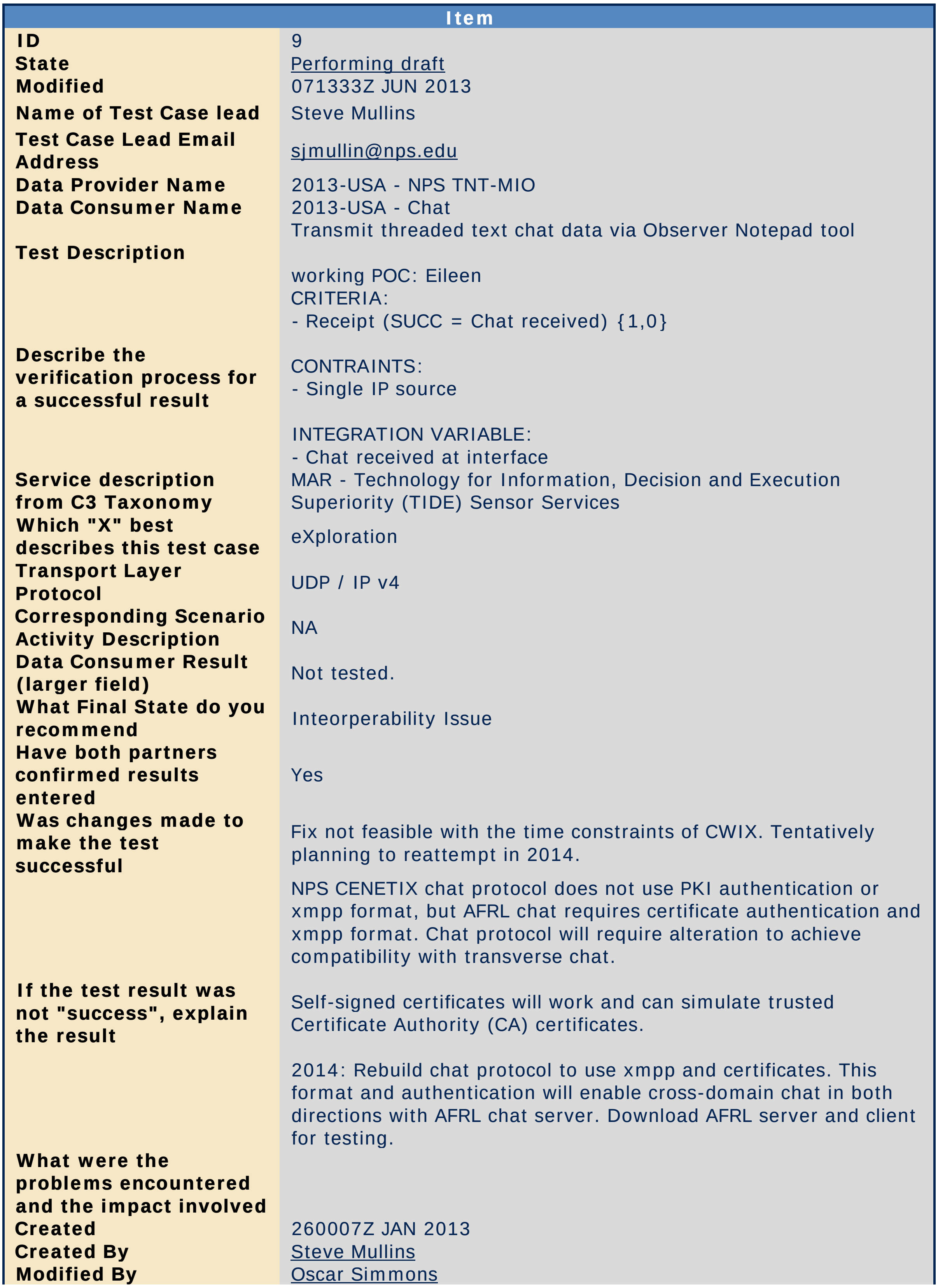
	Track data was passed but the connection between the positions did not transfer. Thus tracks became a collection of unrelated positions with no track line connecting them. The track data transferred correctly; the shortfall was visualizing it.
What Final State do you recommend	Limited Success
Have both partners confirmed results entered	Yes
Was changes made to make the test successful	Custom software written by NPS coder to capture UDP stream and convert to a single CoT XML text file. This file was overwritten with each track update. Custom software written by CMRE coder to read single CoT XML text file every five seconds and write a new CoT XML file named with date and time.
If the test result was not "success", explain the result	CMRE COP did not show track history.
What were the problems encountered and the impact involved	Custom NPS software could not generate a sequence of discreet timestamped XML text files.
Created	260012Z JAN 2013
Created By	Steve Mullins
Modified By	Brian Hillers

Figure 13. Test report for pushing track data (Allied Command Transformation Command & Control Deployability & Sustainability 2013).

Here again the difficulties of cross-domain solutions and differing file formats impeded the collection and display of data. Key to information sharing on a coalition network will be the use of common standards for messaging on all communicating networks.

2. Pushing Chat Cross Domain

A web-based chat application, Observer Notepad (ON), is used for C2 of the TNT MIO experiment. A test goal was to export the content of this dialogue to a higher level of classification for monitoring. As described in Figure 14, two difficulties prevented the test from taking place this year. First, the higher domain requires a PKI certificate for authentication, and certificates are not currently implemented in Observer Notepad. Second, the Extensible Messaging and Presence Protocol (XMPP) format is required by the recipient for the chat messages to be imported. This protocol is one which ON does not support. While this test could not be accomplished during CWIX 2013, the team expects to implement changes to format and inclusion of authentication certificates in next year's testing.



Item	
ID	9
State	Performing draft
Modified	071333Z JUN 2013
Name of Test Case lead	Steve Mullins
Test Case Lead Email Address	sjmullin@nps.edu
Data Provider Name	2013-USA - NPS TNT-MIO
Data Consumer Name	2013-USA - Chat
Test Description	Transmit threaded text chat data via Observer Notepad tool
Describe the verification process for a successful result	working POC: Eileen CRITERIA: - Receipt (SUCC = Chat received) {1,0} CONTRAINTS: - Single IP source INTEGRATION VARIABLE: - Chat received at interface
Service description from C3 Taxonomy	MAR - Technology for Information, Decision and Execution Superiority (TIDE) Sensor Services
Which "X" best describes this test case	eXploration
Transport Layer Protocol	UDP / IP v4
Corresponding Scenario Activity Description	NA
Data Consumer Result (larger field)	Not tested.
What Final State do you recommend	Inteorperability Issue
Have both partners confirmed results entered	Yes
Was changes made to make the test successful	Fix not feasible with the time constraints of CWIX. Tentatively planning to reattempt in 2014.
If the test result was not "success", explain the result	NPS CENETIX chat protocol does not use PKI authentication or xmpp format, but AFRL chat requires certificate authentication and xmpp format. Chat protocol will require alteration to achieve compatibility with transverse chat. Self-signed certificates will work and can simulate trusted Certificate Authority (CA) certificates. 2014: Rebuild chat protocol to use xmpp and certificates. This format and authentication will enable cross-domain chat in both directions with AFRL chat server. Download AFRL server and client for testing.
What were the problems encountered and the impact involved	
Created	260007Z JAN 2013
Created By	Steve Mullins
Modified By	Oscar Simmons

Figure 14. Test report for cross domain chat (Allied Command Transformation Command & Control Deployability & Sustainability 2013).

While useful to the TNT MIO team, Observer Notepad represents a nonstandard format chat tool. This is an element to stay away from in coalition information sharing. Simple functionality, like chat, can be brought to the Koinonia network with a variety of available standard tools that utilize industry standard protocols which aid interoperability.

V. CONCLUSIONS AND RECOMMENDATIONS

A. TYPE OF FRAMEWORK NEEDED

1. Classification

There is no benefit from an unclassified network where a Secret network already exists, as between NATO allies. If CENTRIX or BICES networks already provide the ability to collaborate and share information at the Secret level and below, then those systems can do everything that Koinonia promises, and more. Therefore the types of coalitions with whom the U.S. military would conceivably use a Koinonia network would be those with non-allied partner nations and NGOs with whom a classified network connection does not exist. In such coalitions it may not be possible or even desirable to share classified data. These coalitions would benefit from an enhanced ability to share unclassified information.

The fact that the information exchanged across a network with partners such as these must be unclassified does not mean that it must be unprotected or public. Since we are discussing the exchange of information that could include intelligence and the factor that distinguishes this from other types of information is the necessity of some degree of secrecy (Warner 2002), then clearly unclassified intelligence data would not be public, open, or unprotected from disclosure. The network should then be capable of processing Sensitive but Unclassified information, such as that restricted in distribution to data "For Official Use Only (FOUO)." Despite such data not being classified or marked NOFORN (Not releasable to foreign nationals), it should be protected from unauthorized disclosure, and so there is a necessity for information assurance measures designed to protect it.

Typical procedure is the first item in need of change. The U.S. military's default modus operandi of uploading all ISR data to a classified network is not dictated by policy. If ISR data were put on the domain appropriate to the data's level of classification, as it should be, then expanded sharing of unclassified information becomes feasible. The policy goal for the architecture is consistent with Joint Intelligence doctrine.

> The architecture supporting this type of environment must be dynamic, flexible, and capable of providing multinational partners and interagency participants rapid access to appropriate data. It must facilitate the capability of the Intelligence Community to focus on supporting the JFC and subordinate joint force components and to integrate support from non-DoD agencies and NGOs as needed. (U.S. Department of Defense 2007)

2. Data Transfer

There is no technical constraint that restricts a network intended to share unclassified ISR or C2 data to only that data. An unclassified computer network has the technical capability of sharing any type of data, so rules governing its usage could potentially permit the processing of types of unclassified data beyond its primary or original purpose. For example, unclassified C2 data might easily be shared across the same network. However, routing of traffic with disparate sources, especially material brought from public internet sources, presents a problem. One way to mitigate this is through use of Extensible Markup Language (XML) routing.

XML routing using the N.25 protocol (compliant with the National Information Exchange Model) (NIEM 2010) has a valuable lesson for message interoperability. A message format that is exhaustively large and has data fields for all relevant message types will be able to accept data from any compatible format. Then algorithms can be written for each pair of message formats which need to be exchanged to translate from related fields in the input to the closest corresponding field in the output. In this manner, interoperability can be achieved between systems that rely on dissimilar data formats by means of translation algorithms and a new large, universal format type able to directly accept data from any existing formatting system. This mechanism is illustrated in Figure 15.

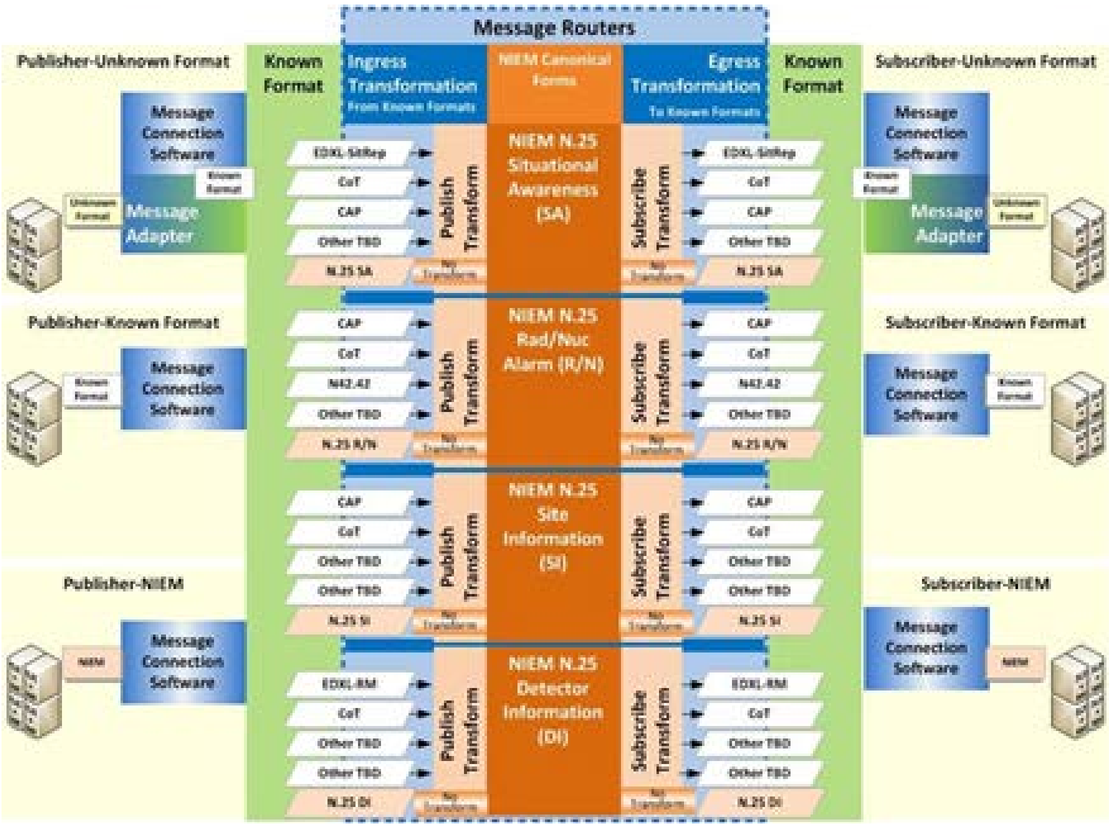


Figure 15. XML routing architecture (From Hall 2012).

3. Applications and Data

An unclassified domain will have access to a plethora of Internet resources that are less easily accessed from classified domains. These include social media sources of publicly available intelligence, like Facebook and Twitter, as well as Google's resources such as Earth and Maps with Street View, or their open and free non-proprietary alternatives, like Open Street Map. It will also permit the use of tools like Ushahidi, which is designed for mobile crowdsourcing, and Sahana, the free and open source disaster management software. Cloud, social, and mobile computing are big trends in IT (Egan 2011). It is desirable that Koinonia take advantage of those increasingly significant areas. APAN is another web-based collaboration portal and toolset being developed by DoD's Defense Information Systems

Agency (DISA) and accessible over the public Internet. (Chlebo, Christman and Johnson 2011).

4. Information Assurance

An unclassified network designed to enable the aggregation and sharing with coalition partners of ISR or C2 data could implement information assurance (IA) controls such as those identified in the NSA's Suite B as appropriate for the protection of classified information. These IA measures are not classified, and the standards and protocols they employ are public. Commercial off-the-shelf (COTS) cryptographic products are available that meet the NSA's requirements, and these would be suitable for use on an unclassified domain (National Security Agency 2009).

B. CAPABILITIES REQUIRED

1. Clarify Requirements for Coalition Data Sharing.

Requirement	**Conclusion**
Purpose/mission	Operations other than war
Classification	Unclassified
Access	Military, Government, NGO, IGO
Duration	Mission length
Mutual Benefit	Collaboration through sharing information
Centralized decision making	Integration for a common operational picture
Trusted network	Information assurance controls
Technology	COTS, XML routing
Data Inputs	Standardized messages
Interoperability	Message format conversion

Table 4. Requirements and Conclusions.

This Koinonia network is designed to address the need for a mission-specific network that need only exist for the duration of the mission. It is a small, tactical network, not a large permanent network. This will permit instances of it to be tailored to the particular set of partners suitable for a given mission. Small size enables inexpensive hardware and software to be used, and permits a network to be rapidly deployable.

Thus the solution is a temporary network that does not compete with large, permanent networks with more extensive capabilities but which are more costly to quickly build in a new environment.

The requirement that it be rapidly deployable for emergent tasking and, for example, usable in the critical early phase of a humanitarian assistance or disaster relief mission, will mean that it is light and transportable. This size limitation from the transportability requirement means that it will only scale up so far. Deployable infrastructure will not support thousands of users.

2. Points of Vulnerability.

Classified networks can employ stringent security measures and control the pool of users that access them, but a network such as Koinonia is designed to by employed between both trusted military users and relatively unknown non-allied foreign military personnel and civilians from regional or international organizations. The degree of security that can be achieved is significantly less. It would probably not be possible, for example, to issue PKI tokens to aid workers from the International Red Cross sufficiently quickly to enable them to use the network effectively within the first 48 hours of a humanitarian crisis. There is no possibility of knowing ahead of time which personnel will require access, and no time to execute the tedious administrative protocols necessary to implement PKI security during an emergency.

Recommendation: A JSOTF or similar small tactical unit needs timely and efficient information sharing, through good business processes using a secure and available network, with enterprise architecture designed to facilitate sharing unclassified information. National security strategy and joint military doctrine recognize the need for increased agility in this area. A JSOTF often conducts missions of limited duration requiring specific capabilities from a wide range of possible requirements. The proposed potential solution set can improve upon the shortfalls of existing business processes and network capabilities.

C. FUTURE WORK

1. Expanded Utility of Data Sharing Beyond ISR or C2

An information exchange system that is capable of sharing ISR data, which often entails full motion video and other bandwidth-intensive products, will probably be suitable for applications other than ISR or C2.

2. Independent Network

The CWIX experimentation relied on a NATO network for collection and dissemination of data. Building the network stack and workstations for a rapidly deployable and affordable mobile network on which to implement Koinonia is a necessary step for practical development and experimentation.

3. Expand Points of Collection

The experiment collected sensor data from dedicated teams of operators. Opening the aperture for collection to other types of information gathering utilizing tools such as Ushahidi, Sahana, and Open Street Maps would demonstrate the utility of an unclassified domain for multinational information sharing.

LIST OF REFERENCES

Ackerman, R K. “Intelligence Center Mines Open Sources.” *Signal*, March 2006: 60–66.

Alberts, David S, and Richard E Hayes. *Planning: Complex Endeavors.* Washington DC: CCRP, 2007.

Ara, Martin J, Thomas Brand, and Larssen Brage A. 2011 “Help a Brother Out: A Case Study and Multinational Intelligence Sharing, NATO SOF, Master’s thesis*.* Naval Postgraduate School.

Aronson, Pratkanis and. *Age of Propaganda.* New York: W. H. Freeman, 1992.

Bordetsky, Alex, and David Netzer. "Testbed for Tactical Networking and Collaboration." Edited by R. Douglas Flournoy. *The International C2 Journal* (CCRP) 4, no. 3 (2010): 1–31.

Cartwright, James E. "Information Sharing is a Strategic Imperative." *CROSSTALK The Journal of Defense Software Engineering* 19, no. 7 (2006): 7-9.

Chisolm, M. "The Twin Towers of Bi Babel." *DM Review*, 2007: 24–28.

Chlebo, Paul Jr, Gerald J Christman, and Roy A Johnson. *Enhancing Collective C2 in the International Environment: Leveraging the Unclassified Information Sharing Enterprise Service.* Arlington: Office of the Assistant Secretary Of Defense (Network and Info Integration), 2011.

Christman, Gerard. "Data sharing in a Stability Operations Community of Interest." *Defense Technical Information Center.* October 28, 2009. Accessed June 3, 2013. http://www.dtic.mil/ndia/2009systemengr/8788WednesdayTrack8Christman.pdf

Christman, GJ. "On Facilitating Stability Operations: a Net Centric, Federated Approach to Information Sharing." *15th International Command and Control Research and Technology Symposium.* Arlington: Office of the Assistant Secretary of Defense for Networks and Information, 2010. 10.

Daniel, J D, K N Goh, and S M Yusop. "Data Transformation Service (DTS) Creating Data." *International Journal of Computer Science & Engineering*, 2007: 207–211.

Director of National Intelligence and Chief Information Officer. *Intelligence Community Classification Guidance Findings and Recommendations*

Report. Government Report, Arlington: Government printing office, 2008.

Dron, Alan. *Special Network—Alliance Aims to Improve Cooperation among Special Operators.* September 1, 2009. Accessed April 22, 2013. http://www.defensenews.com/article/20090901/C4ISR02/909010317/Special-network

Egan, Mark, interview by Prashant Rao. *The Cloud, socialization, and mobile technology will enable CIOs to have a greater impact on business* (October 2011).

Eggers, William. *Case Study: Intelligence-Open Source Data Analytics.* Washington DC: Deloitte, 2012.

Euchner, James. "From the Editor [Special Section]." *Research-Technology Management*, 2010: 7–8.

Flaherty, Anne. *U.S. plans next-gen spy satellite program.* November 30, 2007. Accessed April 22, 2013. http://www.nbcnews.com/id/22046019/#.UXWIA7Xvt8E

Gateau, James, interview by authors. *Combined Endeavor* (December 18, 2012).

Government Accountability Office. *Federal Efforts Are Helping to Alleviate Some Challenges Encountered by State and Local Information Fusion Centers.* Washington DC: Government Printing Office, 2007.

Hammergren, Thomas C, and Allen R Simon. "An Intelligent Look at Business Intelligence." In *Data Warehousing for Dummies (2nd edition)*, by Thomas C Hammergren, 115. Hoboken: Wiley, 2009.

Hester, Vaughn, Aaron Shaw, and Lukas Biewald. "Scalable crisis relief: Crowdsourced SMS translation and categorization with Mission 4636." *Proceedings of the First ACM Symposium on Computing for Development (ACM DEV '10).* New York: ACM, 2010. 7 pages.

International Council on Security and Government. *Afganistan Transition: Missing Variables.* London, UK: ICOS, 2010, 11-13.

Juskalian, Russ. *Interview with Clay Shirky, Part I.* December 19, 2008. Accessed April 23, 2013. http://www.cjr.org/overload/interview_with_clay_shirky_par.php?page=all

McKenna, Corey. *Social Network Adds Situational Awareness to Haitian Earthquake Response.* June 30, 2010. Accessed May 6, 2013. http://www.emergencymgmt.com/safety/Social-Network-Situational-Awareness-Haiti-Earthquake.html

McMullen, Ben S, COL. Interview by authors. Stuttgart, August 24, 2012.

National Security Agency. *NSA Suite B Cryptography.* January 15, 2009. Accessed May 4, 2013. http://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml

NATO. *NATO Allied Command Transformation: CWIX.* 2013. Accessed May 22, 2013.http://www.act.nato.int/mainpages/cwix-2013

News Group. *Social Media & the Arab Spring.* Arab Media Influence Report, Dubai: News Group International, 2011.

NIEM. "The DHS Domestic Nuclear Detection Office Goes NIEM." *National Information Exchange Model.* May 2010. Accessed May 25, 2013. https://www.niem.gov/documentsdb/Documents/Success%20Stories/SuccessStory_DHS.pdf

North Atlantic Treaty Organization Special Operations Coordination Centre. *The North Atlantic Treaty Organization Special Operations Forces Study.* Mons, Belguim: NSCC, 2008.

NPS MDSRP, USSOCOM, DTRA . *NETWORKING AND INTERAGENCY COLLABORATION ON SMALL CRAFT MARITIME-SOURCED NUCLEAR RADIOLOGICAL THREAT DETECTION AND INTERDICTION .* Field Experimentation, Department of Information Science, Naval Postgraduate School, Monterey: Naval Postgraduate School, 2012, 62.

Obama, President Barack. *Strategic Guidance.* Washington, D.C.: United States Government, 2010.

Office of the President of the United States. *National Security Strategy.* Government Strategy Report, Washington DC: Government Printing Office, 2010.

Petraeus, David. *Special Operations Intelligence Branch.* Mons Belgium: NATO Special Operations Headquarters, 2010.

Pincus, Walter. *Intelligence spending at record US$80.1 billion overall.* October 29, 2010. Accessed April 22, 2013. http://www.washingtonpost.com/wp-dyn/content/article/2010/10/28/AR2010102807284.html

President of the United States. *National Security Strategy.* Washington DC: Government Printing Office, 2010.

Reveron, Derek S. "Old Allies, New Friends: Intelligence-Sharing in the War on Terror." *Orbis* 50, no. 3 (Summer 2006): 453–468.

Shirky, Clay, interview by Russ Juskalian. *Interview with Clay Shirky, Part I* (December 19, 2008).

Tempest fact sheet. *Global Security.org.* May 7, 2011. Accessed May 3, 2013. http://www.globalsecurity.org/military/ops/tempest-express.htm

U.S. Department of Defense. *Joint Publication 2-0, Joint Intelligence.* Washington D.C.: Government Printing Office, 2007.

——. *Joint Publication 2-01, Joint and National Intelligence Support to Military Operations.* Washington D.C.: Government Printing Office, 2012.

United States Government Accountability Office. *Federal Efforts Are Helping to Alleviate Some Challenges Encountered by State and Local Information Fusion Centers.* Report to Congressional Committees, Washington DC: Government Accountability Office, 2007.

US Department of Defense. *Joint Publication 3-05.1, Joint Special Operations Task Force Operations.* Washington DC: Government Printing Office, 2007.

Warner, Michael. "Wanted: A Definition of "Intelligence"." *Studies in Intelligence*, 2002: 15–22.

Wells, Linton II, and Khalil Ali. *Crowdsourcing and Collaborative Tools in Virtual Online Disaster Relief Scenarios.* April 20, 2011. http://science.dodlive.mil/2011/04/20/crowdsourcing-and-collaborative-tools-in-virtual-online-disaster-relief-scenario/ (accessed May 6, 2013).

Wills, David R. *Mission Networks: An Evolution in Information Sharing.* Carlisle Barracks: Army War College, 2012.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California